НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

«На правах рукопису»
УДК _____

«До захисту допущено»
Завідувач кафедри
_____ Л.О. Уривський
«___»_____20__ р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Дослідження критеріїв та розробка пропозицій з оцінки безпеки інформаційних технологій»

Виконав (-ла):
студент (-ка) ІІ курсу, групи ТС-з71мп
Клімчук Іван Васильович _____

Керівник:
д.т.н., проф. кафедри
Горицький В. М. _____

Рецензент:
Старший викладач спеціальної кафедри № 5 ІСЗЗІ КПІ ім. Ігоря Сікорського.
Мітін С.В. _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент (-ка) _____

Київ – 2018

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою

Спеціальність (спеціалізація) – 172 «Телекомунікації та радіотехніка» (172.3620.1 «Телекомунікаційні системи та мережі»)

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Л.О. Уривський

«___»_____20__ р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Клімчуку Івану Васильовичу

1. Тема дисертації «Дослідження критеріїв та розробка пропозицій з оцінки безпеки інформаційних технологій», науковий керівник дисертації Горицький Віктор Михайлович, д.т.н., проф. кафедри затверджені наказом по університету від «___»_____ 20__ р. №_____

2. Термін подання студентом дисертації
_____10.12.18_____

3. Об’єкт дослідження: Інформаційна безпека

4. Предмет дослідження: критерії оцінки безпеки інформаційних технологій

5. Перелік завдань, які потрібно розробити

- Побудувати модель оцінки безпеки інформаційних технологій.

- Дослідити функціональні компоненти безпеки інформаційних

технологій.

- Дослідити компоненти довіри до безпеки інформаційних технологій.

6. Орієнтовний перелік графічного (ілюстративного) матеріалу

Аркуш 1 – Взаємозв'язок між вмістом профілю захисту, завданням по безпеці і об'єктом оцінки

Аркуш 2 – Результати оцінки

Аркуш 3 – Приклад декомпозиції функціональних класів

Аркуш 4 – Огляд оціночних рівнів довіри

7. Дата видачі завдання 12.12.2017

Календарний план

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	12.12.2017-15.12.2017	виконано
2	Обгрунтування актуальності теми роботи	15.12.2017-21.02.2018	виконано
3	Написання першого розділу роботи	21.02.2017-11.05.2018	виконано
4	Написання другого розділу роботи	11.05.2018-01.06.2018	виконано
5	Написання третього розділу роботи	01.06.2018-28.08.2018	виконано
6	Написання висновків по роботі	28.08.2018-25.09.2018	виконано
7	Підготовка демонстраційних матеріалів	25.09.2018-23.10.2018	виконано
8	Підготовка доповіді	23.10.2018-27.11.2018	виконано

Студент І.В. Клімчук

Науковий керівник дисертації В.М. Горицький

РЕФЕРАТ

Темою магістерської дисертації є дослідження критеріїв та розробка пропозицій з оцінки безпеки інформаційних технологій

Робота містить 106 сторінок, зокрема 24 ілюстрації, 11 таблиць та 9 джерел інформації.

Тема магістерської дисертації є актуальною, так як інформаційна безпека стає важливим фактором з розвитком інформаційних технологій, несанкціоновані спроби доступу до даних дуже часте явище яке веде до великих втрат.

Мета дисертації полягає в аналізі уже доступних критерії оцінки інформації, аналіз міжнародних стандартів в сфері інформаційної безпеки та розробка рекомендації з оцінки безпеки інформаційних технологій.

Об’єктом дослідження є інформаційна безпека.

Предметом дослідження є критерії оцінки інформаційної безпеки.

При виконанні роботи проводився аналіз доступних рекомендацій по критеріям оцінки безпеки.

У дисертації були запропоновані рекомендації по оцінці інформаційних технологій.

ABSTRACT

The topic of the master's thesis is the study of criteria and the development of proposals for assessing the safety of information technology

The work contains 106 pages, including 24 illustrations, 11 tables and 9 sources of information.

The topic of the master's thesis is relevant, as information security becomes an important factor in the development of information technology, unauthorized attempts to access data is very frequent phenomenon which leads to great losses.

The purpose of the dissertation is to analyze the already available criteria for assessing information, the analysis of international standards in the field of information security and the development of recommendations for assessing the safety of information technology.

The object of research is information security.

The subject of the study is the criteria for assessing information security.

In carrying out the work, an analysis of available recommendations on the criteria for safety assessment.

The dissertation offered recommendations on the evaluation of information technology.

ЗМІСТ

ПЕРЕЛІК ПОСИЛАНЬ

ВПМ (VPN) - віртуальна приватна мережа.

ГІП (GUI) - графічний інтерфейс користувача.

ЗБ (ST) - завдання з безпеки.

ІВК (PKI) - інфраструктура відкритих ключів.

ІС (IC) - інтегральна схема.

ІТ (IT) - інформаційна технологія.

ОО – обєкт оцінки.

ФБО (TSF) - функціональні можливості безпеки ОО.

ФВБ (SFR) - функціональне вимога безпеки.

ВДБ (SAR) - вимога довіри до безпеки.

СПД (CAP) - складовою пакет довіри.

ПФБ (SFP) - політика функції безпеки.

ПЗ (PP) - профіль захисту.

ПБОр (OSP) - політика безпеки організації.

Орд (EAL) - оціночний рівень довіри.

ВПБ (SPD) - визначення проблеми безпеки.

ІФБО (TSFI) - інтерфейс ФБО.

ВСТУП

Всім відомий вислів «Хто володіє інформацією, той володіє світом». А хто володіє інформацією про конкурентів, отримує безпрецедентні переваги в боротьбі з ними. Прогрес зробив компанії залежними від інформаційних систем, а разом з цим - уразливими до атак хакерів, комп'ютерним вірусам, людському і державному фактору в такій мірі, що багато власників бізнесу вже не можуть відчувати себе в безпеці. Питання інформаційної безпеки стає дуже важливим у діяльності організації, але цей же прогрес пропонує рішення, здатні захистити дані від зовнішніх зазіхань.

Що таке інформаційна безпека і чому системи її забезпечення так важливі Так що ж таке інформаційна безпека?

Зазвичай під нею розуміють захищеність інформації і всієї компанії від навмисних або випадкових дій, що призводять до нанесення шкоди її власникам або користувачам. Забезпечення інформаційної безпеки має бути спрямована перш за все на запобігання ризикам, а не на ліквідацію їх наслідків. Саме прийняття запобіжних заходів щодо забезпечення конфіденційності, цілісності, а також доступності інформації і є найбільш правильним підходом у створенні системи інформаційної безпеки.

Будь-який витік інформації може призвести до серйозних проблем для компанії - від значних фінансових збитків до повної ліквідації. Звичайно, проблема витоків з'явилася не сьогодні, промислове шпигунство і переманювання кваліфікованих фахівців існували ще й до епохи комп'ютеризації. Але саме з появою ПК та інтернету виникли нові прийоми незаконного отримання інформації. Якщо раніше для цього необхідно було вкрасти і винести з фірми цілі стоси паперових документів, то зараз величезні обсяги важливих відомостей можна запросто злити на

флешку, що міститься в портмоне, відправити по мережі, вдавшись до використання сімейства троянів, бекдор, кейлоггеров і ботнетів, або просто знищити за допомогою вірусів, влаштувавши диверсію.

Найчастіше «витікають» з компаній документи фінансового характеру, технологічні і конструкторські розробки, логіни і паролі для входу в мережу інших організацій. Але серйозної шкоди може завдати і витік персональних даних співробітників. Особливо це актуально для західних країн, де судові позови через такі витокі нерідко призводять до величезних штрафів, після виплати яких компанії зазнають серйозних збитків.

Інформація, що використовується в системах або продуктах IT, є критичними даними, що дозволяють організаціям успішно вирішувати свої завдання. Також приватні особи мають право надіятись на те, що їх персональна інформація, розміщена в продуктах або системах IT, залишиться приватній, доступної їм у міру необхідності і не буде піддана несанкціонованої модифікації. При виконанні продуктами або системами IT своїх функцій слід здійснювати належне врядування інформацією для забезпечення її захисту від небезпек небажаного або невиправданого поширення, зміни або втрати. Термін "безпека IT" використовується для того, щоб розглянути запобігання і зменшення цих та подібних небезпек.

Багато споживачів IT через нестачу знань, компетентності або ресурсів, не будучи впевнені в безпеці вживаних продуктів і систем IT, можливо, не захочуть покладатися виключно на запевнення розробників. Щоб підвищити свою впевненість в заходах безпеки продукту або системи IT, споживачі можуть замовити проведення аналізу безпеки цього продукту або системи (тобто оцінку безпеки).[1]

ISO / IEC 15408 може використовуватися для вибору прийнятних заходів безпеки IT. У ньому містяться критерії оцінки вимог безпеки.

РОЗДІЛ 1. МОДЕЛЬ ОЦІНКИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

1.1 Загальна модель оцінки безпеки інформаційних технологій

У розділі представлені основні концептуальні положення ISO / IEC 15408. У ньому визначені поняття "ОО", категорії користувачів ISO / IEC 15408, контекст оцінки та загальна модель оцінки.

1.1.1 Об'єкт оцінки

ISO / IEC 15408 є гнучким до того, що оцінюється і таким чином, не прив'язується тільки до продуктів ІТ.

Таким чином в контексті оцінки в ISO / IEC 15408 використовується термін "ОО" (об'єкт оцінки).

ОО визначається як набір програмних, програмно-апаратних та / або апаратних засобів, можливо супроводжуваних посібниками.

Хоча бувають випадки, що ОО є продукт ІТ, це не завжди так. ОО може бути продуктом ІТ, частиною продукту ІТ, набором продуктів ІТ, унікальною технологією, яка може бути ніколи не буде реалізована у вигляді продукту, або поєднанням вище зазначених варіантів.[5]

Щодо ISO / IEC 15408 чітке співвідношення між ОО і будь-якими продуктами ІТ є важливим тільки в одному аспекті: оцінку ОО, що містить частину продукту ІТ, не слід помилково представляти як оцінку продукту ІТ в цілому.

Прикладами ОО є:

- прикладна програма;
- операційна система;
- прикладна програма в поєднанні з операційною системою;

- прикладна програма в поєднанні з операційною системою і робочою станцією;

- операційна система в поєднанні з робочою станцією;

- інтегральна схема смарт-карти;

- локальна обчислювальна мережа, включаючи всі термінали, сервери, мережеве обладнання та програмні засоби;

- додаток бази даних

1.1.1.1 Різні варіанти представлення ОО

В ISO / IEC 15408 ОО може зустрічатися в декількох представленнях, таких як (для програмного ОО):

- список файлів в системі управління конфігурацією;

- окрема копія, яка була тільки що скомпільована;

- коробка, що містить компакт-диск і керівництва, ООтова для постачання споживачеві;

- встановлена і функціональна версія.

1.1.1.2 Різні конфігурації ОО

Зазвичай продукти IT можуть бути налаштовані різними способами шляхом включення або відключення різних опцій при інсталяції. Так як в процесі оцінки по ISO / IEC 15408 визначатиметься, чи задовольняє ОО певним вимогам, дана гнучкість конфігурації може привести до проблем, так як всі можливі конфігурації ОО повинні задовольняти цим вимогам. З цих причин частими є випадки, коли керівництво як частина ОО строго обмежують можливі конфігурації ОО. Таким чином, керівництва ОО можуть відрізнятися від загальних настанов для продукту IT.

Прикладом є продукт IT "Операційна система". Цей продукт може бути налаштований різними способами (наприклад, типи користувачів, кількість користувачів, типи дозволених / недозволених зовнішніх підключень, включення / відключення опцій і ін.)

Якщо такий продукт IT повинен бути ОО і оцінений на відповідність обґрунтованого набору вимог, його конфігурацію слід набагато більш ретельно контролювати, так як багато опції (наприклад, дозвіл всіх типів зовнішніх підключень або відсутність необхідності аутентифікації адміністратора системи) приведуть до того, що ОО НЕ буде задовольняти вимогам.

З цієї причини нормальним б було диференціація посібників для продукту IT (допускають чимало змін) і посібників для ОО (допускають лише одну конфігурацію або тільки ті зміни, які не відрізняються щодо способів забезпечення безпеки).

Якщо керівництва ОО допускають більше однієї конфігурації, то всі ці конфігурації разом іменуються "ГО", і кожна така конфігурація повинна задовольняти вимогам, що пред'являються до ОО. [5]

1.1.2 Користувачі ISO / IEC 15408

В оцінці характеристик безпеки ОО зацікавлені в основному три групи користувачів: споживачі, розробники і оцінювачі. Критерії, представлені в цьому документі, структуровані в інтересах цих груп, тому що саме вони розглядаються як основні користувачі ISO / IEC 15408.

1.1.2.1 Споживачі

ISO / IEC 15408 розроблений, щоб забезпечити за допомогою оцінки задоволення запитів споживачів, оскільки це є основною метою і логічним обґрунтуванням процесу оцінки.

Результати оцінки допомагають споживачам вирішити, чи задовольняє ОО їх потреби в безпеці. Ці потреби зазвичай визначаються як наслідок аналізу ризиків, а також напрямки політики безпеки. Споживачі можуть також використовувати результати оцінки для порівняння різних ОО. Ієрархічне представлення вимог довіри сприяє цьому.

ISO / IEC 15408 надає споживачам, особливо що входять в групи і спільноти з єдиними інтересами, незалежну від реалізації структуру, яка називається профілем захисту (ПЗ), для однозначного виразу їхніх вимог безпеки.

1.1.2.2 Розробники

ISO / IEC 15408 призначений для підтримки розробників при підготовці до оцінки свого ОО і сприяння в її проведенні, а також при встановленні вимог безпеки, яким повинен задовольняти цей ОО. Дані вимоги містяться в залежною від реалізації конструкції, іменованої завданням з безпеки (ЗБ). Ці ЗБ можуть базуватися на одному або декількох ПЗ, щоб показати, що ЗБ відповідають вимогам безпеки, пред'явлених споживачами, які встановлені в даних ПЗ.

ISO / IEC 15408 можна використовувати для визначення обов'язків і дій з надання свідчень, необхідних при проведенні оцінки ОО по цим вимогам. Він також визначає зміст і подання таких свідчень.

1.1.2.3 Оцінювачі

В ISO / IEC 15408 містяться критерії, призначені для використання оцінювачами ОО при формуванні висновку про відповідність об'єктів оцінки пред'явленим до них вимогам безпеки. В ISO / IEC 15408 дається опис сукупності основних дій, які виконуються оцінювачем. При цьому в ISO / IEC 15408 не визначені процедури, яких слід дотримуватися при виконанні цих дій.

1.1.2.4 Інші

Хоча ISO / IEC 15408 орієнтований на визначення і оцінку характеристик безпеки IT для об'єктів оцінки, він також може служити довідковим матеріалом для всіх, хто цікавиться питаннями безпеки IT або несе відповідальність за них. Серед них можна виділити, наприклад, такі групи, представники яких зможуть отримати користь з інформації, наведеної в ISO / IEC 15408:

a) особи, відповідальні за технічний стан обладнання, і співробітники служб безпеки, відповідальні за визначення і виконання політики і вимог безпеки організації в області IT;

b) аудитори як внутрішні, так і зовнішні, відповідальні за оцінку адекватності безпеки IT-рішення (яке може складатися з ОО або включати ОО);

c) проектувальники систем безпеки, відповідальні за характеристики безпеки продуктів IT;

d) відповідальні за приймання IT-рішення в експлуатацію в конкретному середовищі;

e) заявники, які замовляють оцінку і забезпечують її проведення;

f) органи оцінки, відповідальні за керівництво і нагляд за програмами проведення оцінок безпеки ІТ.

1.1.3 Контекст оцінки

Для досягнення більшої порівнянності результатів оцінок їх слід проводити в рамках офіційної системи оцінки, яка встановлює стандарти, контролює якість оцінок і визначає норми, якими необхідно керуватися організаціям, що проводять оцінку, і самим оцінювачам.

В ISO / IEC 15408 (в усіх частинах) немає вимоги до правової бази. Однак узгодженість правової бази різних органів оцінки є необхідною умовою досягнення взаємного визнання результатів оцінок.

Другий напрямок досягнення більшої порівнянності результатів оцінок полягає в використанні загальної методології отримання цих результатів. Для всіх частин ISO / IEC 15408 така методологія наведена в ISO / IEC 18045.

Використання загальної методології оцінки дозволяє досягти повторюваності і об'єктивності результатів, але тільки цього недостатньо. Багато з критеріїв оцінки вимагають залучення експертних рішень і базових знань, домогтися узгодженості яких буває нелегко. Для підвищення узгодженості висновків, отриманих при оцінці, її кінцеві результати можуть бути представлені на сертифікацію.

Процес сертифікації має незалежну експертизу результатів оцінки, яка завершується їх затвердженням або видачею сертифікату. Відомості про сертифікати зазвичай публікуються і є загальнодоступними. Сертифікація є засобом забезпечення більшої узгодженості в застосуванні критеріїв безпеки ІТ.[2]

Системи оцінки і процеси сертифікації знаходяться під наглядом органів оцінки, керуючих системами і процесами оцінки, і не входять в зону дії ISO / IEC 15408 (всіх частин).

1.1.4 Введення до загальної моделі

У цьому розділі представлені загальні поняття, які використовуються у всіх частинах ISO / IEC 15408, включаючи контекст використання цих понять. ISO / IEC 15408-2 і ISO / IEC 15408-3, до яких повинні звертатися користувачі ISO / IEC 15408-1, розвивають ці поняття в рамках описаного підходу. Крім того, тим користувачам ISO / IEC 15408-1, які збираються виконувати види діяльності з оцінки, необхідний ISO / IEC 18045. Даний розділ передбачає наявність певних знань з безпеки IT і не призначений для використання в якості навчального посібника в цій області.

Безпека в ISO / IEC 15408 (в усіх частинах) розглянута з використанням сукупності понять безпеки і термінології. Їх розуміння є передумовою ефективного використання ISO / IEC 15408 (всіх частин). Однак самі по собі ці поняття мають самий загальний характер і не призначені для обмеження класу проблем безпеки IT, до яких застосовується ISO / IEC 15408.

1.1.5 Активи та контрзаходи

Безпека пов'язана із захистом активів. Активи - це сутності, що представляють цінність для кого-небудь. Приклади активів включають:

- зміст файлу або сервера;
- справжність голосів, поданих на виборах;

- доступність процесу електронної комерції;

- можливість використовувати дорогий принтер;

- доступ до засобів обмеженого доступу.

Але так як цінність - це дуже суб'єктивне поняття, то майже все, що завгодно, може розглядатися в якості активів.

Середовище, в якому розміщуються ці активи, називається середовищем функціонування. Прикладами (аспектами) середовища функціонування є:

- комп'ютерне приміщення в банку;

- комп'ютерна мережа, підключена до Інтернету;

- локальна обчислювальна мережа (ЛОМ);

- звичайне офісне середовище.

Багато активів представлені у вигляді інформації, яка зберігається, обробляється і передається продуктами IT таким чином, щоб задовільнити вимоги власників цієї інформації. Власник інформації має право вимагати, щоб доступність, поширення і модифікація будь-якої такої інформації суворо контролювалися і активи були захищені від погроз контрзаходами. рис 1.1.5 ілюструє високорівневі поняття безпеки та їх взаємозв'язок.

Рисунок 1.1.5 Поняття безпеки та їх взаємозв'язок

За збереження розглянутих активів відповідають їх власники, для яких ці активи мають цінність. Існуючі або передбачувані порушники також можуть надавати значення цих активів і прагнути використовувати їх всупереч інтересам їх власника. Прикладами джерел загрози є хакери, зловмисні користувачі, не зловмисні користувачі (які іноді роблять помилки), комп'ютерні процеси і збої.

Власники активів будуть сприймати такі загрози як потенційну можливість нанесення такого збитку активам, при якому цінність активів для власників зменшилася б. Специфічний для безпеки збиток зазвичай полягає в наступному (але не обмежується цим): втрата конфіденційності активів, втрата цілісності активів або втрата доступності активів.

Таким чином, ці загрози збільшують ризики для активів, що залежать від ймовірності реалізації загрози і збитку активам при реалізації даної загрози. Для того щоб зменшити ризики для активів, реалізуються контрзаходи. Ці контрзаходи можуть включати IT-контрзаходи (такі як міжмережеві екрани і смарт-карти) і не-IT-контрзаходи (такі як охорона і процедури).

Оскільки за активи можуть нести (несуть) відповідальність їх власники, то їм слід мати можливість відстоювати своє рішення про прийнятність ризику для активів, створюваного погрозами.

При відстоюванні цього рішення повинна бути можливість продемонструвати два важливих моменти, що:

- контрзаходи є достатніми, якщо контрзаходи виконують те, що заявлено, і загрозам, спрямованим на активи, забезпечується протистояння;

- контрзаходи є коректними, якщо контрзаходи виконують те, що заявлено.

Багато власників активів не мають знань, досвіду та ресурсів, необхідних для винесення судження про достатність і коректності контрзаходів, і при цьому вони можуть не захотіти покладатися виключно на затвердження розробників цих контрзаходів. Внаслідок цього дані споживачі можуть захотіти підвищити свою впевненість в достатності і правильності деяких або всіх контрзаходів шляхом замовлення оцінки цих контрзаходів.

Рис 1.1.5.1 ілюструє поняття, використовувані при оцінці і їх взаємозв'язок.

Рисунок 1.1.5.1 Поняття, що використовуються при оцінці, і їх взаємозв'язок

1.1.6 Достатність контрзаходів

При оцінці достатність контрзаходів аналізується через конструкцію, звану завданням з безпеки.

Завдання з безпеки починається з опису активів і загроз цим активам. Потім в завданні з безпеки описуються контрзаходи (в формі цілей безпеки) і демонструється, що дані контрзаходи є достатніми, щоб протистояти описаним загрозам: якщо контрзаходи здійснюють те, що заявлено по відношенню до них, то забезпечено протистояння загрозам.

Далі в завданні з безпеки контрзаходи діляться на дві групи:

a) цілі безпеки для ОО: вони описують контрзаходи, коректність яких буде визначатися при оцінці;

b) цілі безпеки для середовища функціонування: вони описують контрзаходи, коректність яких не буде визначатися при оцінці.

Причинами даного поділу є:

- ISO / IEC 15408 застосуємо тільки для оцінювання коректності контрзаходів ІТ. Отже, не-ІТ-контрзаходи (наприклад, співробітники служби безпеки, процедури) завжди відносять до середовища функціонування;

- оцінювання коректності контрзаходів вимагає витрат часу і грошей, можливо роблячи неможливою оцінку коректності всіх контрзаходів ІТ;

- коректність деяких контрзаходів ІТ може бути вже оцінена в ході іншої оцінки. Отже, економічно неефективно проводити їх повторну оцінку.

У завданні з безпеки для ОО (коректність контрзаходів ІТ якого будуть оцінювати в процесі оцінки) потрібна подальша деталізація цілей безпеки для ОО в функціональних вимогах безпеки (ФТБ). Ці ФВБ

формулюють на стандартній мові (описаний у ISO / IEC 15408-2), щоб забезпечити точність і полегшити порівняння.

Таким чином, в завданні з безпеки демонструється, що:

- ФВБ задовольняють цілям безпеки для ОО;

- цілі безпеки для ОО та цілі безпеки для середовища функціонування протистоять загрозам;

-отже ФВБ і цілі безпеки для середовища функціонування протистоять загрозам.

З цього випливає, що коректний ОО (задовольняє ФВБ) в поєднанні з коректною середовищем функціонування (задовольняє цілям безпеки для середовища функціонування) буде протистояти загрозам.

1.1.7 Коректність ОО

Об'єкт оцінки може бути неправильно спроектований і реалізований і таким чином може містити помилки, які ведуть до вразливостей. За допомогою використання цих вразливостей, порушники можуть завдати шкоди.

Ці уразливості можуть бути результатом випадкових помилок, зроблених протягом розробки, неналежного проектування, навмисного впровадження шкідливого коду, неналежного тестування та ін.

Для визначення коректності ОО можуть виконуватися різні види діяльності, такі як:

- тестування ОО;

- дослідження різних проектних уявлень ОО;

- дослідження фізичної безпеки середовища розробки ОО.

Завдання з безпеки забезпечує структурований опис цих видів діяльності для визначення коректності в формі вимог довіри до безпеки

(ВДБ). Ці ВДБ формулюються на стандартній мові (описаній в ISO / IEC 15408-3), щоб забезпечити точність і полегшити порівняння.

Якщо ВДБ задовольняються, то існує довіра до коректності ОО, і, таким чином, менше ймовірність, що ОО містить уразливості, які можуть бути використані порушником. Величина довіри, яке існує по відношенню до коректності ОО, визначається самими ВДБ: кілька "слабких" ВДБ приведуть до малої довіри, велике число "сильних" ВДБ призведе до більшої довірі. [5]

1.1.8 Коректність середовища функціонування

Середовище функціонування також може бути неправильно спроектоване і реалізоване і може таким чином, містити помилки, які ведуть до вразливостей. За допомогою використання цих вразливостей, порушники можуть завдати шкоди і несанкціоновано використовувати активи.

Однак в ISO / IEC 15408 довіра не набувається при розгляді коректності середовища функціонування.

Що стосується оцінки, то передбачається, що навколишнє середовище функціонування є на 100% правильним відображенням цілей безпеки для середовища функціонування.

Це не заважає споживачеві ОО використовувати інші методи визначення коректності конкретного середовища функціонування, такі як:

- якщо для ОО типу "ОС" встановлені цілі безпеки для середовища функціонування: "Середовище функціонування повинне забезпечити, щоб сутності з недовірених мережі (наприклад, Інтернету) можуть здійснювати доступ до ОО тільки по ftp", тоді споживач міг би вибрати оцінений

міжмережевий екран і налаштувати його так, щоб до ОО був дозволений доступ тільки по ftp;

- якщо для ОО встановлені цілі безпеки для середовища функціонування: "Середовище функціонування повинне забезпечити, щоб ніхто з усього адміністративного персоналу не буде вести себе зловмисно", тоді споживач міг би адаптувати свої контракти з адміністративним персоналом для включення штрафних санкцій за зловмисну поведінку, але це рішення не є частиною оцінки відповідно до ISO / IEC 15408.

1.1.9 Оцінка

За стандартом ISO / IEC 15408 визнають два типи оцінки: оцінка ЗБ / ОО і оцінка ПЗ. Багато разів в ISO / IEC 15408 використаний термін "оцінка" (без уточнень) для посилання на оцінку ЗБ / ОО. [9]

За ISO / IEC 15408 оцінка ЗБ / ОО проходить в два етапи:

a) оцінка ЗБ: на цьому етапі визначають достатність ОО і середовища функціонування;

b) оцінка ОО: на цьому етапі визначають коректність ОО; як зазначалося раніше, оцінка ОО не включає оцінку коректності середовища функціонування.

Оцінка ОО є більш комплексною. Основні вихідні дані для оцінки ОО: свідоцтва оцінки, які включають ОО і ЗБ, а також, як правило, вихідні дані, одержувані з середовища розробки, такі як проектна документація або результати тестування розробником.

Оцінка ОО полягає в застосуванні ВДБ (із завдання з безпеки) до свідчень оцінки. Конкретний спосіб застосування конкретного ТДБ визначається використовуваної методологією оцінки.

Як документувати результати застосування ВДБ, які звіти необхідно генерувати і в якій мірі деталізації - визначається відповідно до використовуваної методологією оцінки та відповідно до вимог системи оцінки, в рамках якої виконується оцінка.

Результатом процесу оцінки ОО буде:

- твердження, що не всі ВДБ задоволені, і тому не досягнуть заданий рівень довіри до того, що ОО задовольняє ФВБ, які викладені в ЗБ;

- твердження, що все ВДБ задоволені, і тому досягнутий заданий рівень довіри до того, що ОО задовольняє ФВБ, які викладені в ЗБ.

Оцінка ОО може бути виконана після завершення розробки ОО або паралельно з розробкою ОО. [3]

1.2 Доопрацювання вимог безпеки для конкретного застосування

1.2.1 Операції

Функціональні компоненти і компоненти довіри з ISO / IEC 15408 можна використовувати точно так, як вони сформульовані в ISO / IEC 15408-2 і ISO / IEC 15408-3, або ж можна їх конкретизувати, застосовуючи дозволені операції. При використанні операцій розробник ПЗ / ЗБ повинен також відстежити, щоб залежно інших вимог, які залежать від цієї вимоги, були задоволені. Дозволені операції вибирають з наступної сукупності:

a)ітерація (iteration): дозволяє неодноразово використовувати компонент при різному виконанні в ньому операцій;

b)призначення (assignment): дозволяє визначати параметри;

c)вибір (selection): дозволяє вибирати один або більше пунктів з переліку;

d)уточнення (refinement): дозволяє здійснювати деталізацію.

Операції "призначення" і "вибір" дозволені тільки в тих місцях компонента, де вони спеціально позначені. Операції "призначення" і "вибір" дозволені для всіх компонентів.

Додатки ISO / IEC 15408-2 надають керівництво по допустимому виконання операцій вибору і призначення. Це керівництво надає нормативні інструкції по тому, як виконувати операції, і цим інструкціям необхідно слідувати, якщо розробник ПЗ / ЗБ логічно й доведе відхилення від цих інструкцій:

a)"Ні" допускається як варіант виконання вибору тільки якщо він явно передбачений.

Списки, передбачені для виконання операцій вибору, не повинні бути порожніми. У разі вибору параметра "Ні", не можуть бути обрані ніякі інші додаткові варіанти. Якщо "Ні" не передбачено в якості варіанту вибору, допускається поєднання варіантів в операції вибору з союзами "і" і "або", якщо в операції вибору в явному вигляді не визначено "вибрати одне з".

Операції вибору при необхідності можна поєднувати з ітерацією. У цьому випадку застосування обраного варіанту для кожної ітерації не повинно перетинатися з предметом іншої ітерації вибору, так як вони повинні бути унікальними.

b)По відношенню до виконання операцій призначення необхідно звернутися до додатків ISO / IEC 15408-2, щоб визначити, коли "Ні" є допустимим виконанням.

1.2.1.1 Операція "ітерація"

Операція "ітерація" може бути виконана по відношенню до будь-якого компонента. Розробник ПЗ / ЗБ виконує операцію "ітерація" шляхом

включення в ПЗ / ЗБ кількох вимог, заснованих на одному і тому ж компоненті. Кожна ітерація компонента повинна відрізнятися від усіх інших ітерацій цього компонента, що реалізується завершенням по-іншому операцій "призначення" і "вибір" або застосуванням по-іншому операції "уточнення".

Різні ітерації слід унікально ідентифікувати, щоб забезпечити чітке обгрунтування та простежуваності від або до цих вимог.

У ряді випадків операція "ітерація" може бути виконана по відношенню до компоненту, для якого замість його ітерації можна було б виконати операцію "призначення", вказавши діапазон або список значень. В цьому випадку розробник ПЗ / ЗБ може вибрати найбільш підходящу альтернативу, вирішивши з урахуванням всіх обставин, чи є потреба надання єдиного обгрунтування для всього діапазону значень або необхідно мати окреме обгрунтування для кожного із значень. Розробнику також слід звернути увагу на те, чи потрібно окреме простежування для цих значень.

1.2.1.2 Операція "призначення"

Операцію "призначення" здійснюють тоді, коли розглядається компонент який включає елемент з деяким параметром, значення якого може бути встановлено розробником ПЗ / ЗБ. Параметром може бути нічим не обмежена змінна або правило, яке обмежує змінну конкретним діапазоном значень.

Кожен раз, коли елемент в ПЗ передбачає операцію "призначення", розробник ПЗ повинен виконати одну з чотирьох дій:

а)залишити операцію "призначення" повністю невиконаною. Розробник ПЗ, наприклад, міг би включити в ПЗ "При досягненні або

перевищенні певного числа неуспішних спроб аутентифікації ФБО повинні виконати призначенний: список дій":

b)повністю виконати операцію "призначення". Наприклад, розробник ПЗ міг би включити в ПЗ "При досягненні або перевищенні певного числа неуспішних спроб аутентифікації ФБО повинні запобігати в подальшому прив'язку відповідної зовнішньої сутності до якогось суб'єкту";

c)обмежити операцію "призначення", щоб в подальшому обмежити діапазон допустимих значень. Наприклад, розробник ПЗ міг би включити в ПЗ "ФБО повинні виявити, коли станеться [призначення: натуральне число від 4 до 9] неуспішних спроб аутентифікації ...";

d)перетворити "призначення" в "вибір", обмежуючи таким чином "призначення". Наприклад, розробник ПЗ міг би включити в ПЗ FIA_AFL.1.2 "При досягненні або перевищенні певного числа неуспішних спроб аутентифікації ФБО повинні [вибір: запобігати в подальшому прив'язку відповідного користувача до якомусь суб'єкту, повідомляти адміністратора"].

1.2.1.3 Операція "вибір"

Операцію "вибір" здійснюють тоді, коли розглядається компонент включає елемент, в якому розробником ПЗ / ЗБ повинен бути зроблений вибір з кількох пунктів.

Кожен раз, коли елемент в ПЗ передбачає операцію "вибір", розробник ПЗ може виконати одну з трьох дій:

a)залишити операцію "вибір" повністю невиконаної;

b)повністю виконати операцію "вибір" шляхом вибору одного або більше пунктів;

с)обмежити операцію "вибір", видаливши деякі з варіантів, але залишивши два або більше.

1.2.1.4 Операція "уточнення"

Операція "уточнення" може бути виконана по відношенню до будь-якої вимоги. Розробник ПЗ / ЗБ виконує уточнення шляхом зміни вимоги. Перше правило по відношенню до уточнення полягає в тому, щоб ОО, що задовільняє вимогу, також задовільняв неуточнений мимогу в контексті ПЗ / ЗБ (тобто уточнена вимога повинна бути "більш важливою", ніж вихідна вимога). Якщо уточнення не задовільняє цьому правилу, то результуюча уточнена вимога вважається розширенею вимогою і буде розглядатися як така.

Єдиний виняток з цього правила полягає в тому, що допускається, щоб розробник ПЗ / ЗБ уточнив ФВБ для його застосування по відношенню до деяких, але не до всіх суб'єктів, об'єктів, операціями, атрибутам безпеки і / або зовнішнім сутностей.

1.2.2 Залежності між компонентами

Між компонентами можуть існувати залежності. Залежно виникають, коли компоненти не самодостатній і передбачає наявність іншого компонента для забезпечення функціональних можливостей безпеки або довіри до безпеки.

Функціональні компоненти в ISO / IEC 15408-2 зазвичай мають залежності від інших функціональних компонентів, також як деякі компоненти довіри в ISO / IEC 15408-3 можуть мати залежності від інших компонентів ISO / IEC 15408-3. Можуть бути також визначені залежності

компонентів з ISO / IEC 15408-2 від компонентів з ISO / IEC 15408-3. Не виключено також наявність залежностей розширених функціональних компонентів від компонентів довіри або навпаки.

Опис залежностей компонентів визначається з урахуванням визначень компонентів в ISO / IEC 15408-2 і ISO / IEC 15408-3. Щоб забезпечити повноту вимог до ОО, слід задовольнити залежності компонентів при включенні в ПЗ і ЗБ вимог, заснованих на компонентах, що мають залежності. Залежності слід також враховувати при формуванні пакетів.

Іншими словами, якщо компонент А має залежність від компонента Б, це означає, що коли ПЗ / ЗБ містить вимогу безпеки, засноване на компоненті А, ПЗ / ЗБ повинен також містити одну з таких дій:

а)вимога безпеки, засноване на компоненті Б;

b)вимога безпеки, засноване на компоненті, більш високому по ієрархії по відношенню до Б;

c)обгрунтування, чому ПЗ / ЗБ не містить вимоги безпеки, заснованого на компоненті Б.

У випадках a) і b), коли вимога безпеки включено внаслідок наявності залежності, може бути необхідним виконати операції (призначення, ітерація, уточнення, вибір) по відношенню до цієї вимоги безпеки таким чином, щоб забезпечити впевненість у тому, що воно дійсно задовольняє залежність . [5]

1.2.3 Розширені компоненти

Згідно ISO / IEC 15408 необхідно, щоб вимоги грунтувалися на компонентах з ISO / IEC 15408-2 або ISO / IEC 15408-3 з двома винятками:

a)існують цілі безпеки для ОО, які не можуть бути перетворені в ФВБ з ISO / IEC 15408-2, або існують вимоги "третьої сторони" (наприклад, закони, стандарти), які не можуть бути перетворені в ВДБ з ISO / IEC 15408-3 (наприклад, пов'язані з оцінкою криптографії);

b)мітки безпеки можуть бути виражені на основі компонентів з ISO / IEC 15408-2 і / або ISO / IEC 15408-3, але тільки з великими труднощами і / або складнощами.

В обох випадках від розробника ПЗ / ЗБ потрібно визначити власні компоненти. Ці певні компоненти називаються розширеними компонентами. Певний розширений компонент необхідний для забезпечення контексту і значення розширених ФВБ або ВДБ, заснованих на цьому компоненті.

1.3 Профілі захисту і пакети

Щоб дати можливість зацікавленим групам або співтовариствам споживачів висловлювати свої потреби безпеки і полегшити розробку ЗБ, дана частина ISO / IEC 15408 надає дві спеціальні конструкції: пакети і профілі захисту (ПЗ

1.3.1 Пакети

Пакет - це іменований набір вимог безпеки. Пакети діляться на:

- функціональні пакети, що включають тільки ФВБ;
- пакети довіри, що включають тільки ВДБ.

Змішані пакети, що включають як ФВБ, так і ВДБ, не припустимі.

Пакет може бути визначений якою-небудь стороною і призначений для багаторазового використання. Для цієї мети він повинен включати вимоги, які в поєднанні є корисними і ефективними.

Пакети можуть використовуватися при створенні більших пакетів, ПЗ і ЗБ. В даний час не існує критеріїв оцінки пакетів, тому будь-який набір ФВБ або ВДБ може бути пакетом.

Прикладами пакетів довіри є оціночні рівні довіри (Орд).

1.3.2 Профілі захисту

У той час як ЗБ завжди описує конкретний ОО (наприклад, міжмережевий екран Х-2, версія 3.1), ПЗ призначений для опису типу ОО (наприклад, міжмережеві екрани прикладного рівня). Тому один і той же ПЗ можна використовувати в якості шаблону для безлічі різних ЗБ, які будуть використовувати в різних оцінках.

Зазвичай ЗБ описує вимоги для ОО та його формує розробник ОО, в той час як ПЗ описує загальні вимоги для деякого типу ОО і тому зазвичай розробляється:

- спільнотою користувачів, які прагнуть прийти до консенсусу щодо вимог для даного типу ОО;

- розробником ОО або групою розробників подібних ОО, які бажають встановити мінімальний базис для конкретного типу ОО;

- урядовою організацією або великою корпорацією, що визначають свої вимоги як частина процесу закупівлі.

ПЗ визначає допустимий тип відповідності ЗБ профілем захисту. Тобто в ПЗ встановлюють, які типи відповідності є допустимими для ЗБ, а саме:

- якщо в ПЗ встановлено, що потрібно "сувора відповідність", то ЗБ має в суворій формі відповідати ПЗ;

- якщо в ПЗ встановлено, що потрібно "демонструється відповідність", то ЗБ має або строго відповідати ПЗ, або його відповідність ПЗ може бути продемонстровано.

Іншими словами, для ЗБ допускається "демонструється відповідність" ПЗ, тільки якщо ПЗ в явному вигляді це дозволяє.

Якщо в ЗБ заявляють про відповідність кільком ПЗ, то воно повинно відповідати (як описано вище) кожному з цих ПЗ в такій формі, як це вказано в цьому ПЗ. Це має на увазі, що ЗБ може строго відповідати одним ПЗ і демонстрований відповідати іншим ПЗ.

Завдання з безпеки або відповідає розглянутому ПЗ, або не відповідає. ISO / IEC 15408 не визнає "часткову" відповідність. Тому обов'язок розробника ПЗ - забезпечити, щоб ПЗ НЕ був надмірно перевантаженим і не створював би, таким чином, перешкод розробникам ПЗ / ЗБ при заяві про відповідність ПЗ.

ЗБ еквівалентно ПЗ або є більш обмежувальним, якщо:

- ОО, який задовольняє ЗБ, також задовольняє ПЗ;

- все середовища функціонування, які задовольняють ПЗ, також задовольняють ЗБ.

Простіше кажучи, ЗБ повинен накласти ті ж самі або великі обмеження на ОО і ті ж самі або менші обмеження на середу функціонування ОО.

Це загальне твердження може бути більш конкретизовано для різних підрозділів ЗБ:

Визначення проблеми безпеки: обгрунтування відповідності в ЗБ має продемонструвати, що визначення проблеми безпеки в ЗБ є

еквівалентним (або більш обмежувальним) по відношенню до визначення проблеми безпеки в ПЗ. Це означає, що:

- ОО, який би відповідав визначенню проблеми безпеки в ЗБ, також відповідав би визначенню проблеми безпеки в ПЗ;

- всі середовища функціонування, які відповідали б визначенню проблеми безпеки в ПЗ, також відповідали б визначенню проблеми безпеки в ЗБ. [5]

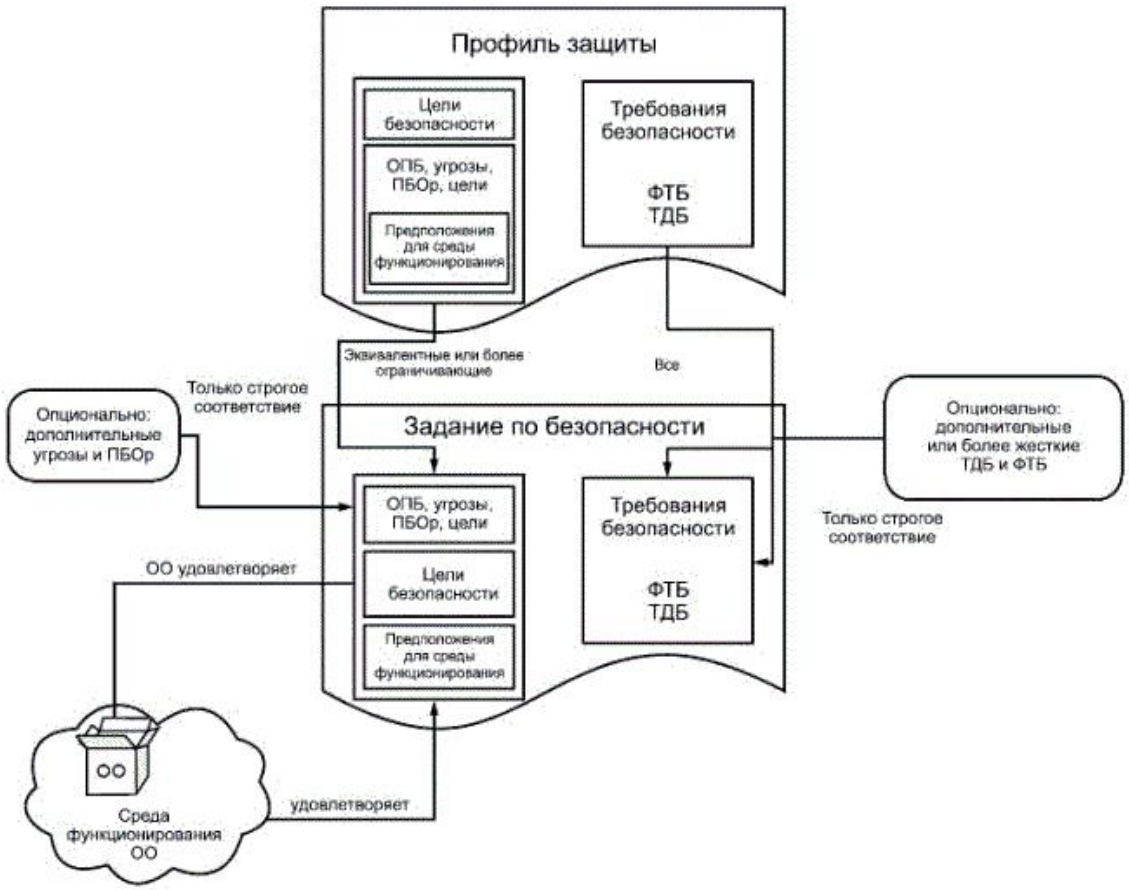

Рисунок 1.3 Взаємозв'язок між вмістом ПЗ, ЗБ і ОО

1.3.3 Використання ПЗ і пакетів

Якщо в ЗБ затверджується про відповідність одному або більше пакету і / або профілем захисту, оцінка даного ЗБ буде (серед інших характеристик даного ЗБ) демонструвати, що ЗБ дійсно відповідає цим

пакетам і / або ПЗ, по відношенню до яких затверджується про відповідність.

Це робить можливим наступний процес:

a) організація, зацікавлена в придбанні конкретного типу продукту безпеки ІТ, викладає свої потреби в безпеці в ПЗ, потім забезпечує його оцінку і випуск;

b) розробник отримує цей ПЗ, розробляє ЗБ, яке містить твердження про відповідність даного ПЗ, і забезпечує оцінку цього ЗБ;

c) потім розробник створює ОО (або використовує існуючий) і забезпечує його оцінку на відповідність ЗБ.

В результаті розробник може довести, що його ОО задовольняє потребам в безпеці організації: тому організація може закупити цей ОО. Аналогічний порядок може застосовуватися щодо пакетів.

1.3.4 Багаторазове використання профілів захисту

ISO / IEC 15408 також допускає відповідність профілів захисту іншим ПЗ, передбачаючи створення ланцюжків профілів захисту, в яких кожен наступний ПЗ базується на попередньому (попередніх) ПЗ.

Наприклад, можна було б взяти ПЗ для інтегральної схеми і ПЗ для ОС смарт-карти і використовувати їх для розробки ПЗ для смарт-карти, в якому стверджується про відповідність двом вихідним ПЗ. Потім можна було б розробити ПЗ для смарт-карт для громадського транспорту, базуючись на ПЗ для смарт-карт і ПЗ для завантажується в них програми. В кінцевому рахунку, розробник міг би потім розробити ЗБ, базуючись на цьому ПЗ для смарт-карт для громадського транспорту.

1.4 Результати оцінки

У цьому розділі представлені очікувані результати оцінки ПЗ і ЗБ:

- оцінки профілів захисту дозволяють створювати каталоги (реєстри) оцінених ПЗ;

- оцінка ЗБ дає проміжні результати, які потім використовуються при оцінці ОО;

- оцінки ЗБ / ОО дозволяють створювати каталоги (реєстри) оцінених ОО. У багатьох випадках ці каталоги будуть посилатися на продукти ІТ, на основі яких визначені ці ОО, а не на конкретні ОО. Отже, наявність продукту ІТ в каталозі не повинно інтерпретуватися як ознака того, що весь продукт ІТ пройшов оцінку; реальний обсяг оцінки ЗБ / ОО визначається ЗБ.

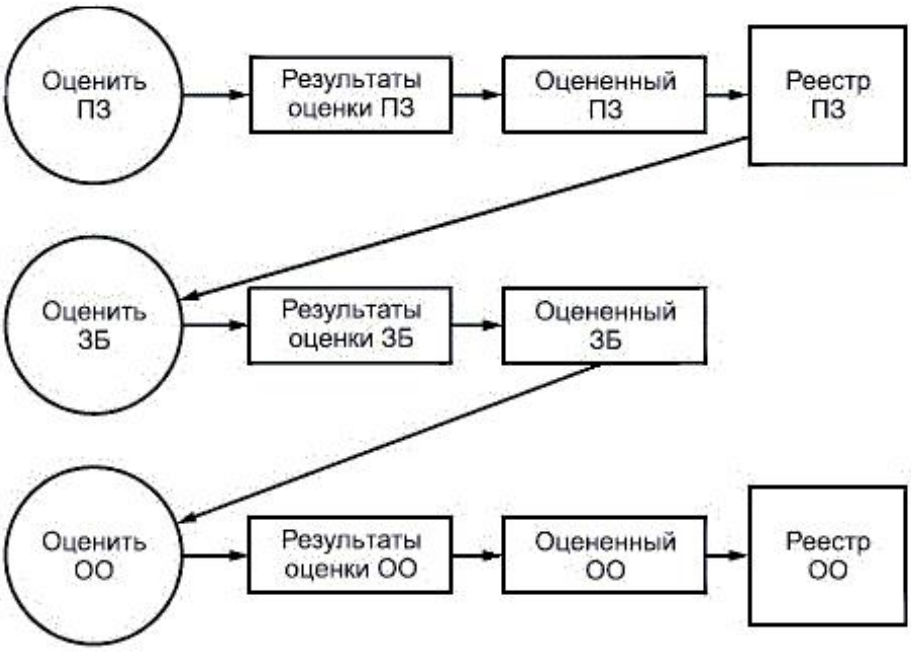

Рисунок 1.4 Результати оцінки

ЗБ можуть базуватися на пакетах, оцінених ПЗ, неоцінених ПЗ; проте, зовсім не обов'язково, щоб ЗБ на чимось базувалися.

Необхідно, щоб оцінка приводила до об'єктивних і повторюваним результатами, на які потім можна посилатися як на свідчення навіть при відсутності абсолютно об'єктивної шкали для представлення результатів оцінки безпеки ІТ. Наявність сукупності критеріїв оцінки є необхідною попередньою умовою для того, щоб оцінка приводила до значимого результату, надаючи технічну основу для взаємного визнання результатів оцінки різними органами оцінки.

Результатом оцінки є підсумкові дані специфічного типу дослідження характеристик безпеки ОО. Такий результат не гарантує придатність до використання в будь-якої конкретної середовищі застосування. Рішення про приймання ОО до використання в конкретному середовищі застосування грунтується на обліку багатьох аспектів безпеки, включаючи і висновки оцінки.

1.4.1 Результати оцінки ПЗ

ISO / IEC 15408-3 містить критерії оцінки, які оцінювачу необхідно взяти до уваги для того, щоб встановити, чи є ПЗ повним, несуперечливим, технічно правильним і отже, придатним для використання при розробці ЗБ.

1.4.2 Результати оцінки ЗБ / ОО

ISO / IEC 15408-3 містить критерії оцінки, які оцінювачу необхідно взяти до уваги для того, щоб встановити, чи існує достатня довіра до того, що ОО задовольняє ФВБ з ЗБ.

Результат оцінки ОО повинен формулюватися як "відповідність / невідповідність" по відношенню до ЗБ. Якщо і для ЗБ, і для ОО результат оцінки - "відповідає", то відповідний продукт отримує право включення до реєстру.

Можливо, результати оцінки в подальшому будуть використані в процесі сертифікації, але цей процес знаходиться за рамками ISO / IEC 15408.

1.4.3 Затвердження про відповідність

Затвердження про відповідність вказує джерело сукупності вимог, яким задовольняє ПЗ або ЗБ, що проходять оцінку. Це твердження про відповідність містить твердження про відповідність ISO / IEC 15408, який:

a)описує ту версію ISO / IEC 15408, про відповідність якої заявлено в ПЗ або ЗБ;

b)описує відповідність ISO / IEC 15408-2 (функціональні вимоги безпеки), що включає одну з таких дій:

- "відповідність ISO / IEC 15408-2" - ПЗ або ЗБ відповідає ISO / IEC 15408-2, якщо все ФВБ в даному ПЗ або ЗБ засновані тільки на функціональних компонентах з ISO / IEC 15408-2;

- "розширення ISO / IEC 15408-2" - ПЗ або ЗБ є розширеним по відношенню до ISO / IEC 15408-2, якщо як мінімум одне ФВБ в даному ПЗ або ЗБ не грунтується на функціональних компонентах з ISO / IEC 15408-2;

c)описує відповідність ISO / IEC 15408-3 (вимоги довіри до безпеки), що включає одну з таких дій:

- "відповідність ISO / IEC 15408-3" - ПЗ або ЗБ відповідає ISO / IEC 15408-3, якщо всі ВДБ в даному ПЗ або ЗБ засновані тільки на компонентах довіри з ISO / IEC 15408-3;

- "розширення ISO / IEC 15408-3" - ПЗ або ЗБ є розширеним по відношенню до ISO / IEC 15408-3, якщо як мінімум одна ВДБ в даному ПЗ або ЗБ не грунтується на компонентах довіри з ISO / IEC 15408-3.

- "відповідність іменованого пакету" - ПЗ або ЗБ. [5]

1.4.4 Використання результатів оцінки ЗБ / ОО

Після оцінки ЗБ і ОО у власників активів є довіра (як визначено в ЗБ) до того, що ОО разом із середовищем функціонування протистоять конкретним загрозам. Результати оцінки можуть бути використані власником активів при прийнятті рішення про прийняття ризику, пов'язаного з схильністю активів впливу конкретних загроз.

При цьому власник активів повинен ретельно перевірити наступне:

- чи відповідає визначення проблеми безпеки в ЗБ конкретній проблемі безпеки власника активів;

- чи відповідає середовище функціонування у власника активів (або може бути забезпечено її відповідність) цілям безпеки для середовища функціонування, описаним в ЗБ.

1.5 Висновки з розділу 1

На цьому етапі оцінюють рівень гарантування безпеки інформаційного середовища об'єкта автоматизації на основі оцінки, за якої після виконання рекомендованих заходів можна довіряти інформаційному середовищу об'єкта.

Базові положення цієї методики припускають, що ступінь гарантування залежить від ефективності зусиль, докладених до оцінювання безпеки. Збільшення цих зусиль означає:

- значну кількість елементів інформаційного середовища об'єкта, що беруть участь у процесі оцінювання;

- розширення типів проектів і описів деталей виконання під час проектуванні системи гарантування безпеки;

- суворість проведення робіт, яка полягає у застосуванні більшої кількості інструментів пошуку і методів виявлення менш очевидних слабких місць або зменшення вірогідності їх наявності.

Загалом розглянута вище методика дає змогу оцінити або переоцінити поточний стан інформаційної безпеки підприємства, виробити рекомендації щодо її гарантування (підвищення), знизити потенційні втрати підприємства (організації) підвищенням стійкості функціонування корпоративної мережі, розробити концепцію і політику безпеки підприємства, а також запропонувати плани захисту його конфіденційної інформації, що передається відкритими каналами зв'язку, захисту інформації підприємства від умисного спотворення (руйнування), несанкціонованого доступу до неї, її копіювання або використання. [5]

РОЗДІЛ 2. ДОСЛІДЖЕННЯ ФУНКЦІОНАЛЬНИХ КОМПОНЕНТІВ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

В даному розділі приведена парадигма функціональних вимог безпеки справжнього стандарту. Деякі ключові поняття парадигми показані на рисунках 2.1 і 2.2. Також описані інші, не показані на рисунках ключові поняття.

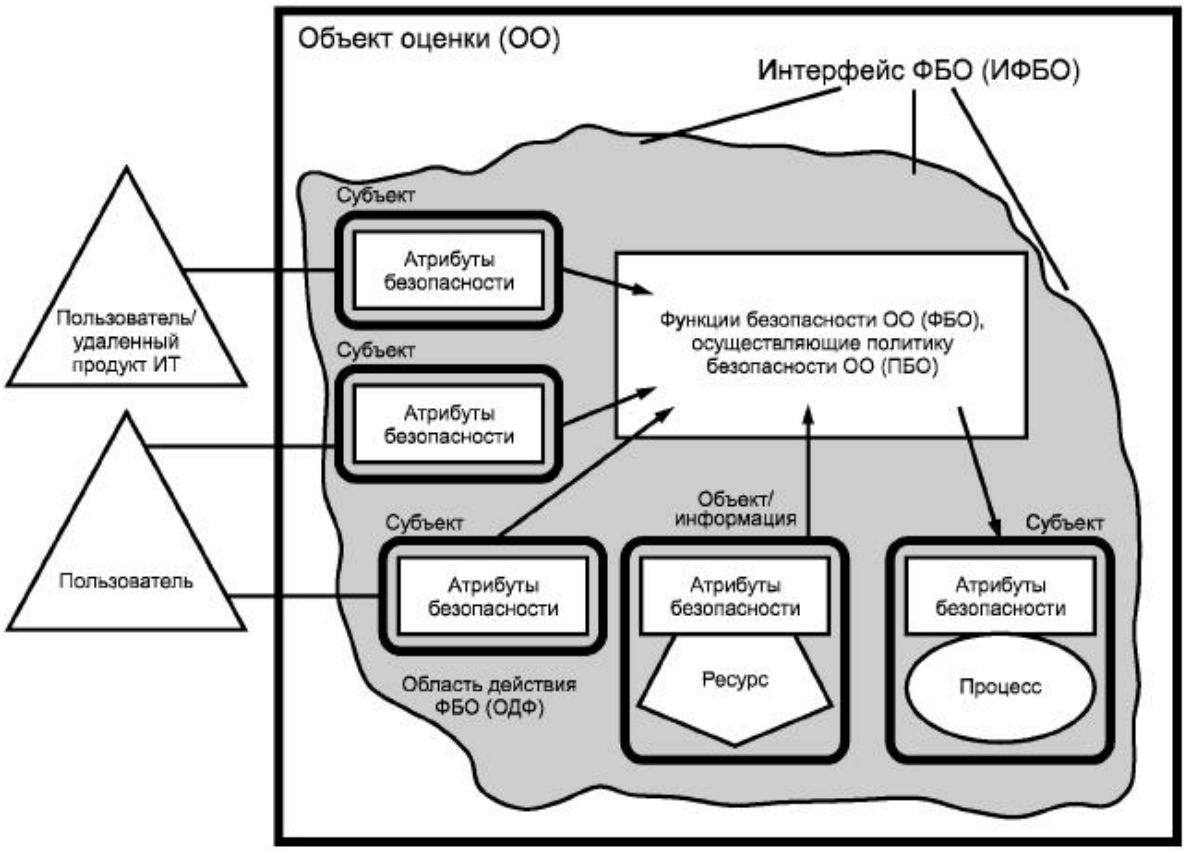

Рисунок 2.1 Ключові поняття функціональних вимог безпеки (єдиний ОО)

Цей стандарт містить каталог функціональних вимог безпеки, які можуть бути пред'явлені до об'єкта оцінки (ОО). ОО - це продукт або система, що містить ресурси типу електронних носіїв даних (таких, як диски), периферійних пристроїв (таких, як принтери) і обчислювальних

можливостей (таких, як процесорний час), які можуть використовуватися для обробки і зберігання інформації і є предметом оцінки. [6]

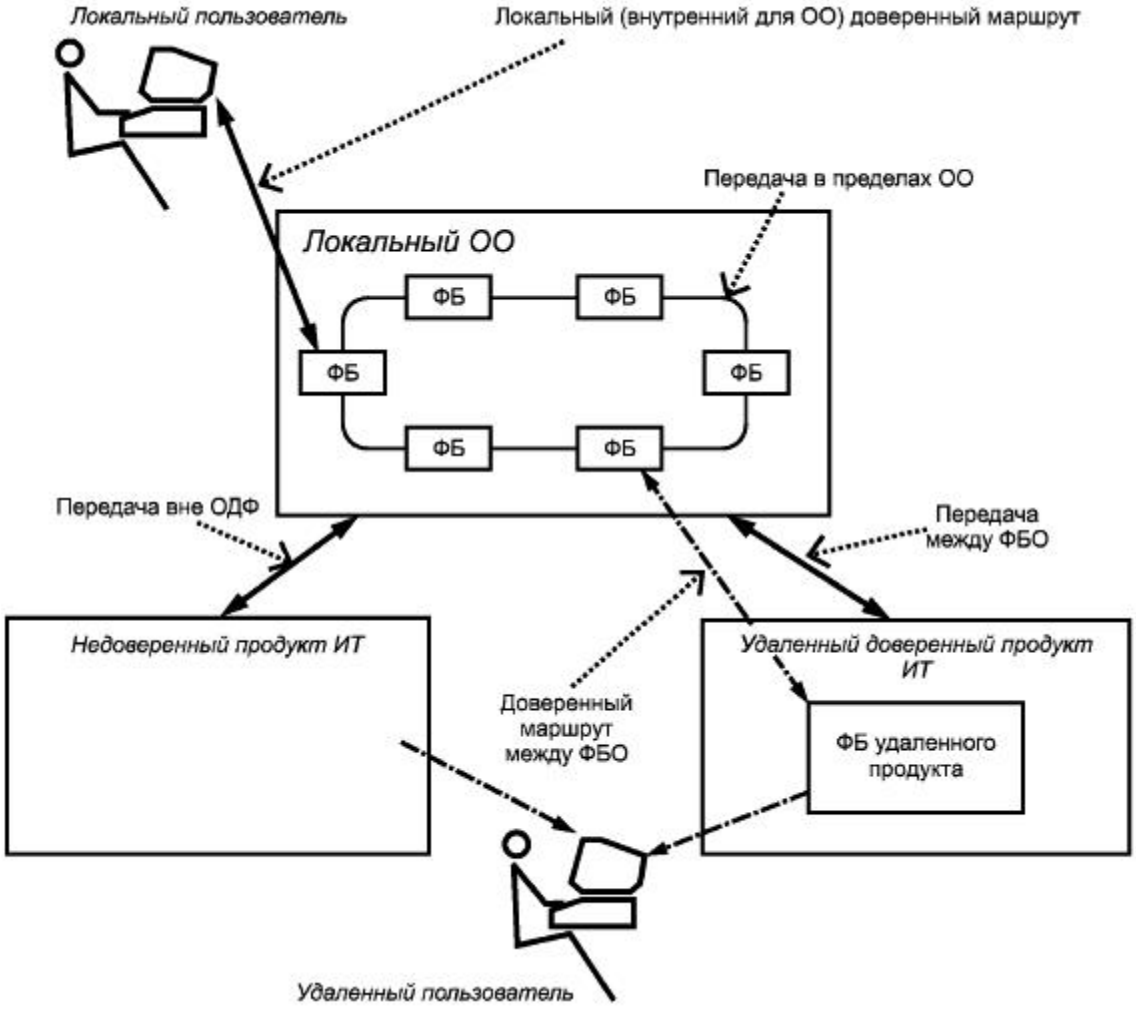

Рисунок 2.2 Функції безпеки в розподіленому ОО

Оцінка насамперед підтверджує, що стосовно ресурсів ОО здійснюється певна політика безпеки ОО (ПБО). ПБО визначає правила, за якими ОО управляє доступом до своїх ресурсів і, таким чином, до всієї інформації та сервісів, контрольованим ОО.

ПБО в свою чергу складається з різних політик функцій безпеки (ПФБ). Кожна ПФБ має свою область дії, що визначає суб'єкти, об'єкти і

операції, на які поширюється ПФБ. ПФБ реалізується функцією безпеки (ФБ), чиї механізми здійснюють політику і надають необхідні можливості.

Сукупність усіх функцій безпеки ОО, які спрямовані на здійснення ПБО, визначаються як функції безпеки об'єкта оцінки (ФБО). ФБО об'єднують функціональні можливості всіх апаратних, програмних і програмно-апаратних засобів ОО, на які як безпосередньо, так і опосередковано покладено забезпечення безпеки.

ОО може бути єдиним продуктом, що включає в себе апаратні, програмно-апаратні і програмні засоби.

В іншому випадку ОО може бути розподіленим, що складається з декількох розділених частин. Кожна частина ОО забезпечує виконання конкретного сервісу для ОО та взаємодіють з іншими частинами ОО через внутрішній канал зв'язку. Цей канал може бути всього лише шиною процесора, а може бути внутрішньою мережею для ОО.

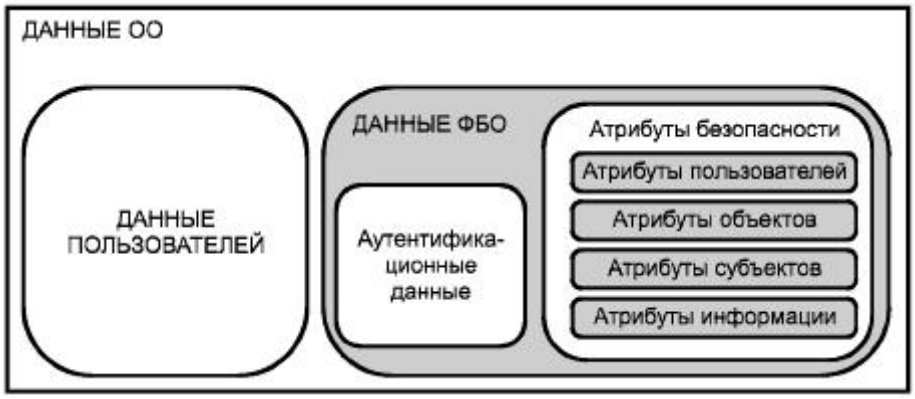

Рисунок 2.3 Зв'язок між даними користувачів та даними ФБО

2.1 Аналіз структур функціональних класів-сімейств-компонентів

2.1.1 Структура класу

Структура функціонального класу наведена на рисунку 2.1.1. Кожен функціональний клас містить ім'я класу, представлення класу і одне або кілька функціональних сімейств.

Рисунок 2.1.1 Структура функціонального класу

2.1.2 Ім'я класу

Ім'я класу містить інформацію, необхідну для ідентифікації функціонального класу і віднесення його до певної категорії. Кожен функціональний клас має унікальне ім'я. Інформація про категорії надана коротким ім'ям, що складається з трьох букв латинського алфавіту. Коротке ім'я класу використовують при завданні коротких імен сімейств цього класу.

2.1.3 Подання класу

Подання класу узагальнює участь сімейств класу в досягненні цілей безпеки. Визначення функціональних класів не відображає формальну таксономію в специфікації вимог.

2.1.4 Структура сімейства

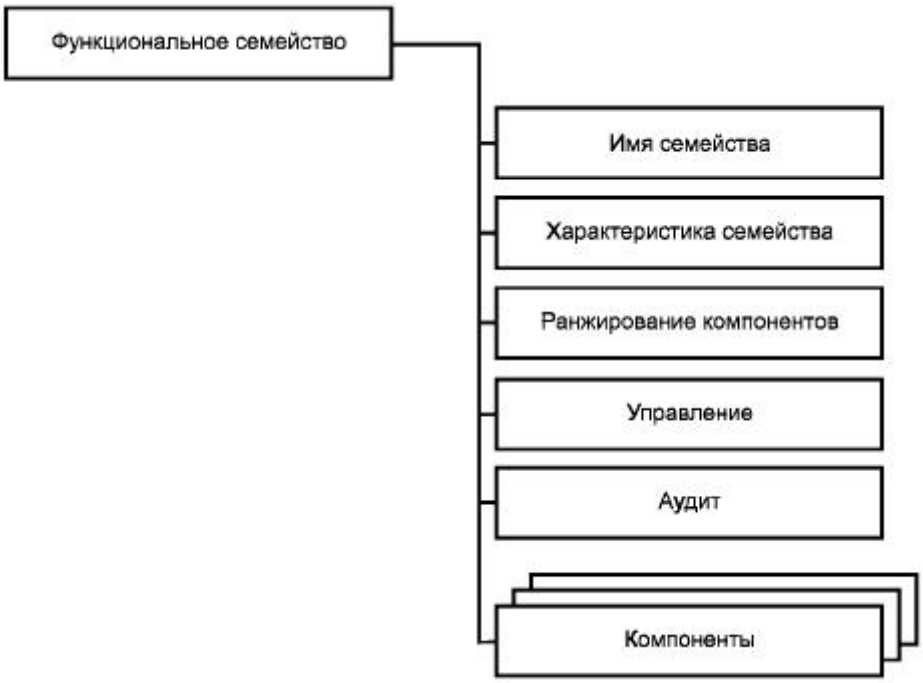

Рисунок 2.5 Структура функціонального сімейства

2.1.5 Ім'я сімейства

Ім'я сімейства містить описову інформацію, необхідну для ідентифікації та категоріювання функціонального сімейства. Кожне функціональне сімейство має унікальне ім'я. Інформація про категорії складається з короткого імені, що включає в себе сім символів. Перші три символи ідентичні короткому імені класу, далі йдуть символ підкреслення і коротке ім'я сімейства у вигляді XXX_YYY. Унікальна коротка форма імені сімейства надає основне ім'я посилання для компонентів.

2.1.6 Характеристика сімейства

Характеристика сімейства - це опис функціонального сімейства, в якому викладаються його цілі безпеки і загальний опис функціональних вимог. Більш детально вони описані нижче:

a) цілі безпеки сімейства характеризують задачу безпеки, яка може бути вирішена за допомогою компонентів цього сімейства;

b) опис функціональних вимог узагальнює всі вимоги, які включені в компоненти). Опис орієнтований на розробників ПЗ, ЗБ і функціональних пакетів, які хотіли б визначити, чи відповідає сімейство їх конкретним вимогам. [6]

2.1.7 Ранжування компонентів

Функціональні сімейства містять один або кілька компонентів, кожен з яких може бути обраний для включення в ПЗ, ЗБ і функціональні пакети. Мета ранжирування компонентів - надати користувачам інформацію для вибору підходящого функціонального компонента, коли буде той дім ідентифіковано користувачем як необхідна або корисна частина вимог безпеки.

Далі перераховуються наявні компоненти і наводиться їх обгрунтування. Деталізація компонентів здійснюється в описі кожного компонента.

Зв'язки між компонентами в межах функціонального сімейства можуть бути ієрархічними і неієрархічні. Компонент важливіший якщо розташований вище по ієрархії по відношенню до іншого компоненту, якщо пропонує більшу безпеку.

Описи сімейств містять графічне представлення ієрархії компонентів.

2.1.8 Управління

Вимоги управління містять інформацію для розробників ПЗ / ЗБ, що враховується при визначенні дій з управління для даного компонента. Вимоги управління деталізовані в компонентах класу "Управління безпекою" (FMT).

Розробник ПЗ / ЗБ може вибрати зазначені вимоги управління або включити нові, не зазначені в цьому стандарті. В останньому випадку має бути подано необхідну інформацію.

2.1.9 Аудит

Вимоги аудиту містять події, потенційно піддаються аудиту, для їх відбору розробниками ПЗ / ЗБ за умови включення в ПЗ / ЗБ вимог з класу FAU "Аудит безпеки". Ці вимоги включають в себе події, які стосуються безпеки, стосовно до різних рівнів деталізації, підтримуваним компонентами сімейства FAU_GEN "Генерація даних аудиту безпеки". Наприклад, запис аудиту будь-якого механізму безпеки може включати в себе на різних рівнях деталізації дії, які розкриваються в наступних термінах:

- мінімальний - успішне використання механізму безпеки;

- базовий - будь-яке використання механізму безпеки, а також інформація про поточні значення атрибутів безпеки;

- деталізований - будь-які зміни конфігурації механізму безпеки, включаючи параметри конфігурації до і після зміни.

Слід врахувати, що категорування подій, потенційно піддається аудиту, завжди ієрархічно. Наприклад, якщо обрана базова генерація даних аудиту, то всі події, ідентифіковані як потенційно піддаються аудиту

і тому входять як в "мінімальну", так і в "базову" записи, слід включити в ПЗ / ЗБ за допомогою відповідної операції призначення, за винятком випадку, коли подія більш високого рівня має більш високий рівень деталізації, ніж подія нижчого рівня, і може просто замінити його. Якщо необхідна деталізована генерація даних аудиту, то всі ідентифіковані події, потенційно піддаються аудиту (для мінімального, базового і детального рівнів), слід включити в ПЗ / ЗБ.

Правила управління аудитом більш докладно пояснені в класі FAU "Аудит безпеки".

2.1.10 Структура компонента

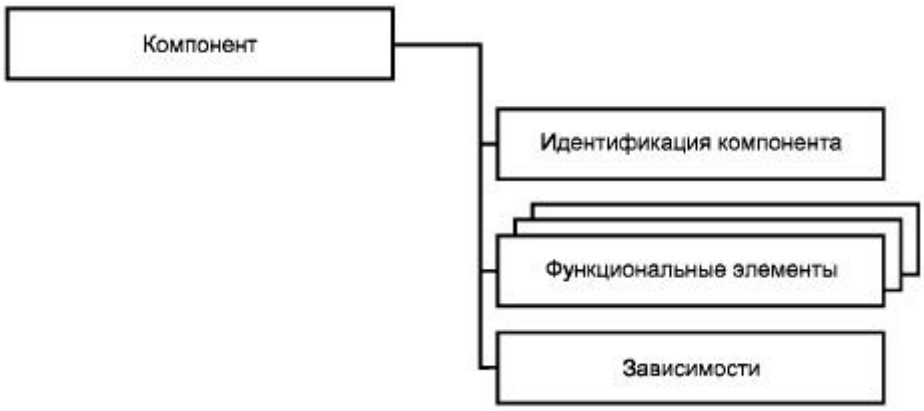

Рисунок 2.1.10 Структура функціонального компонента

Ідентифікація компонента містить у собі описову інформацію, необхідну для ідентифікації, категорування, записи і реалізації перехресних посилань компонента. Для кожного функціонального компонента представляються:

- унікальне ім'я, що відбиває призначення компонента;

- коротке ім'я, яке використовується як основне ім'я посилання для категорування, записи і реалізації перехресних посилань компонента і

унікально відображає клас і сімейство, яким компонент належить, а також номер компонента в сімействі;

- список ієрархічних зв'язків, що містить імена інших компонентів, для яких цей компонент ієрархічний і замість яких може використовуватися при задоволенні залежності від перерахованих компонентів.

2.1.11 Функціональні елементи

Кожен компонент включає в себе набір елементів. Кожен елемент визначається окремо і є самодостатнім.

Функціональний елемент - це функціональне вимога безпеки, подальший поділ якого не змінює значимо результат оцінки; є найменшим функціональним вимогам безпеки, які можуть бути ідентифіковані та визнаним в ISO / IEC 15408. [6]

При формуванні ПЗ, ЗБ або пакетів не дозволяється вибирати тільки частину елементів компонента. Для включення в ПЗ, ЗБ або пакет необхідно вибирати всю сукупність елементів компонента.

Вводиться унікальна коротка форма імені функціонального елемента. Наприклад, ім'я FDP_IFF.4.2 читається так: F - функціональна вимога, DP - клас "Захист даних користувача", _IFF - сімейство "Функції управління інформаційними потоками", .4 - четвертий компонент "Часткове усунення невирішених інформаційних потоків", .2 - другий елемент компонента.

2.1.12 Залежності

Залежно серед функціональних компонентів виникають, якщо компонент не самодостатній і потребує функціональних можливостей іншого компонента або у взаємодії з ним для підтримки власного виконання.[8]

Кожен функціональний компонент містить повний список залежностей від інших функціональних компонентів і компонентів довіри. Для деяких компонентів вказано, що залежностей немає. Компоненти зі списку можуть, в свою чергу, мати залежності від інших компонентів. Список, наведений в компоненті, показує прямі залежності, тобто містить посилання тільки на функціональні компоненти, свідомо необхідні для забезпечення виконання даного компонента. У деяких випадках залежність вибирають з декількох запропонованих функціональних компонентів, причому кожен з них достатній для задоволення залежності (див., Наприклад, FDP_UIT.1 "Цілісність переданих даних").

Список залежностей ідентифікує мінімум функціональних компонентів або компонентів довіри, необхідних для задоволення вимог безпеки, асоційованих з даним компонентом. Компоненти, які ієрархічні по відношенню до компоненту зі списку, також можуть бути використані для задоволення залежності.

Залежності між компонентами, зазначені в цьому стандарті, обов'язкові. Їх необхідно задовольнити в ПЗ / ЗБ. У деяких, особливих випадках ці залежності задовільнити неможливо. Розробник ПЗ / ЗБ, обов'язково обгрунтувавши, чому дана залежність не застосовується, може не включати відповідний компонент в пакет, ПЗ або ЗБ.

2.2 Каталог компонентів

Розташування компонентів в цьому стандарті не відображає будь-яку формальну таксономію.

Цей стандарт містить класи, що складаються з родин і компонентів, які згруповані на основі загальної функції і призначення. Класи і сімейства впорядковані відповідно до латинського алфавіту. На початку кожного класу представлений малюнок, що показує таксономію кожного класу, перераховуючи сімейства в кожному класі і компоненти в кожному сімействі. На малюнку також представлена ієрархія компонентів всередині кожного сімейства.

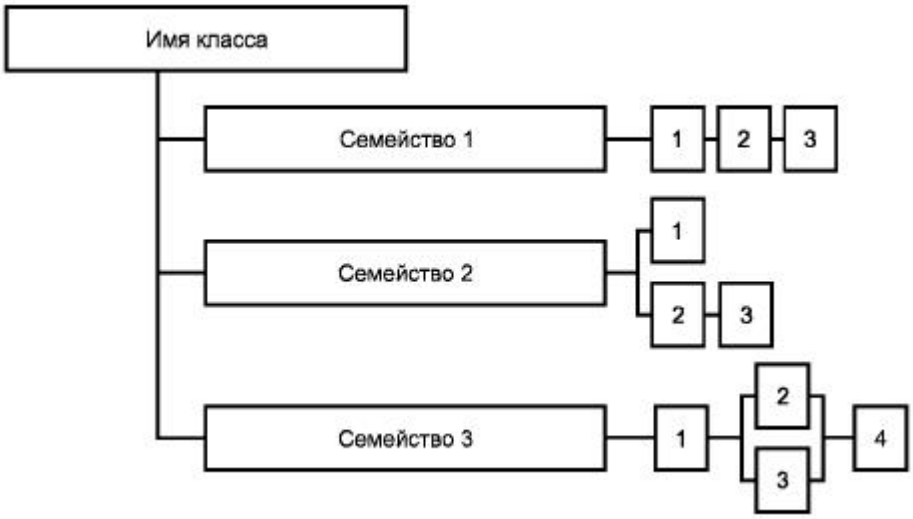

Рисунок 2.2 Приклад декомпозиції класу

У прикладі перша родина містить три ієрархічних компоненти, де компоненти 2 і 3 можуть бути застосовані для виконання залежностей замість компоненту 1. Компонент 3 ієрархічний компоненту 2 і може застосовуватися для виконання залежності замість компонента 2.

У сімействі 2 є три компоненти, не всі з них ієрархічно пов'язані. Компоненти 1 і 2 цієї статті не ієрархічні інших компонентів. Компонент 3 ієрархічний компоненту 2 і може застосовуватися для задоволення залежностей замість компонента 2, але не замість компонента 1.

2.2.1 Клас FAU. аудит безпеки

Аудит безпеки включає в себе розпізнавання, запис, збереження та аналіз інформації, пов'язаної з діями, що стосуються безпеки (наприклад, з діями, контрольованими ПБО). Записи аудиту, одержувані в результаті, можуть бути проаналізовані з тим, щоб визначити, які дії, пов'язані з безпекою, відбувалися, і хто з користувачів за них відповідає.

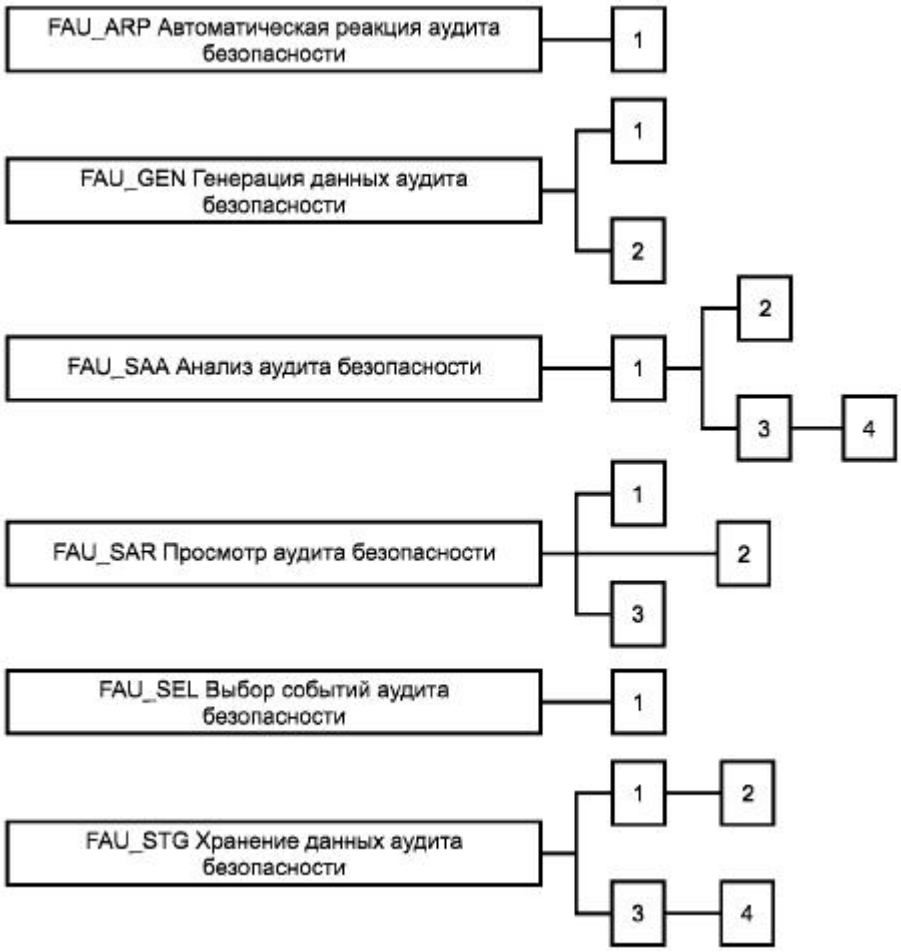

Рисунок 2.2.1 - Декомпозиція класу FAU "Аудит безпеки"

2.2.2 Генерація даних аудиту безпеки (FAU_GEN)

Сімейство FAU_GEN визначає вимоги до реєстрації виникнення подій, що відносяться до безпеки, які підконтрольні ФБО. Дане сімейство ідентифікує рівень аудиту, перераховує типи подій, які потенційно повинні піддаватися аудиту з використанням ФБО, і визначає мінімальний обсяг пов'язаної з аудитом інформації, яку слід подавати в записах аудиту різного типу.

-FAU_GEN.1 "Генерація даних аудиту" визначає рівень подій, потенційно піддаються аудиту, і склад даних, який повинен бути зареєстрований в кожному записі.

У FAU_GEN.2 "Асоціація ідентифікатора користувача" ФБО повинні асоціювати події, потенційно піддаються аудиту, і особисті ідентифікатори користувачів.

2.3 Аналіз функціональних класів

2.3.1 Характеристика сімейства

Сімейство FAU_SAA визначає вимоги для автоматизованих засобів, які аналізують показники функціонування системи і дані аудиту з метою пошуку можливих або реальних порушень безпеки. Цей аналіз може використовуватися для підтримки як виявлення проникнення, так і автоматичної реакції на очікуване порушення безпеки. [6]

Дії, що вживаються при виявленні порушень, можуть бути при необхідності визначені з використанням сімейства FAU_ARP "Автоматична реакція аудиту безпеки".

2.3.2 Ранжування компонентів

У FAU_SAA.1 "Аналіз потенційного порушення" потрібно базовий поріг виявлення на основі встановленого набору правил.

У FAU_SAA.2 "Виявлення аномалії, засноване на профілі" ФБО підтримують окремі профілі використання системи, де профіль являє собою шаблони передісторії використання, що виконувалися учасниками цільової групи профілю. Цільова група профілю може включати в себе одного або декількох учасників (наприклад, окремий користувач; користувачі, спільно використовують загальний ідентифікатор або загальні облікові дані, користувачі, яким призначена одна роль, і всі

2.4 Висновки з розділу 2

Даний стандарт поширюється на функціональні компоненти безпеки, які є основними для функціональних вимог безпеки інформаційних технологій (ІТ) об'єкта оцінки (ОО), викладені в профілі захисту (ПЗ) або в задачі по безпеці (ЗБ). Вимоги описують бажаний безпечний режим функціонування ОО і призначені для досягнення цілей безпеки, встановлених в ПЗ або ЗБ. Вимоги описують також властивості безпеки, які користувачі можуть виявити при безпосередній взаємодії з ОО (тобто при вході і виході) або при реакції ОО на запити.

Функціональні компоненти безпеки виражають вимоги безпеки, спрямовані на протистояння небезпеки в запропонованій середовищі експлуатації ОО та / або охоплюючи будь-яку ідентифіковану політику безпеки організації та припущення.

Даний стандарт призначений для споживачів, розробників, а також оцінювачів безпечних систем та продуктів ІТ

Користувачі - при виборі компонентів для вираження функціональних вимог, що дозволяють задовольнити цілі безпеки, виражені в ПЗ або ЗБ.

Розробники, що несуть відповідальність за виконання існуючих або передбачуваних вимог безпеки споживача при розробці ОО, - для реалізації стандартизованого методу розуміння цих вимог, використовуючи зміст справжнього стандарту як основу для подальшого визначення функцій і механізмів безпеки ОО, які відповідають цим вимогам. [4]

РОЗДІЛ 3. ДОСЛІДЖЕННЯ КОМПОНЕНТІВ ДОВІРИ ДО БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

3.1 Вимоги довіри до безпеки

Наступні пункти описують конструкції, які використовуються в поданні класів, сімейств і компонентів довіри.

На рисунок 3.1 показані вимоги довіри, певні в ISO / IEC 15408-3. Найбільш узагальнена сукупність вимог довіри називається класом. Кожен клас містить сімейства довіри, які розділені на компоненти довіри, що містять, в свою чергу, елементи довіри. Класи і сімейства використовуються для забезпечення систематизації класифікуються вимог довіри, в той час як компоненти застосовуються для специфікації вимог довіри в ПЗ / ЗБ.

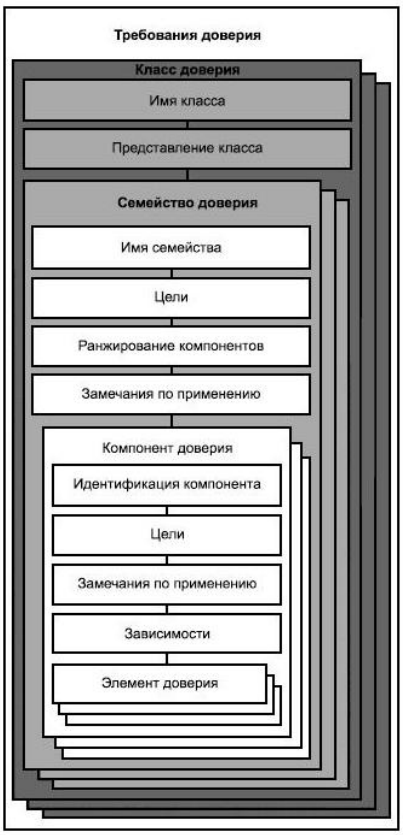

Рисунок 3.1 Ієрархічна структура представлення вимог довіри: клас-сімейство-компонент-елемент

3.1.1 Структура класу

Малюнок 3.1 ілюструє структуру класу довіри.

3.1.1.1 Ім'я класу

Кожному класу довіри присвоєно унікальне ім'я. Ім'я вказує на тематичні розділи, на які поширюється даний клас довіри.

Представлена також унікальна коротка форма імені класу довіри. Вона є основним засобом для посилання на клас довіри. Прийняте умовне позначення включає в себе букву "A", за якою слідують ще дві букви латинського алфавіту, що відносяться до імені класу. [7]

3.1.1.2 Подання класу

Кожен клас довіри має вступний підрозділ, в якому описані склад і призначення класу.

3.1.2 Сімейства довіри

Кожен клас довіри містить, щонайменше, одну родину довіри.

Кожному сімейству довіри присвоєно унікальне ім'я. Ім'я містить описову інформацію за тематичними розділами, на які поширюється дане сімейство довіри. Кожне сімейство довіри розміщено в межах класу довіри, який містить інші сімейства тієї ж спрямованості.

Представлена також унікальна коротка форма імені сімейства довіри. Вона є основним засобом для посилання на сімейство довіри.

Прийняте умовне позначення включає в себе коротку форму імені класу і символ підкреслення, за яким слідують три букви латинського алфавіту, що відносяться до імені сімейства.

3.1.2.1 Цілі

Підрозділ "Цілі" сімейства довіри представляє призначення сімейства довіри.

У ньому описані цілі, для досягнення яких призначене сімейство, особливо пов'язані з парадигмою довіри ISO / IEC 15408. Опис цілей для сімейства довіри представлено в загальному вигляді. Будь-які конкретні подробиці, необхідні для досягнення цілей, включені в конкретний компонент довіри.

3.1.2.2 Ранжування компонентів

Кожне сімейство довіри містить один або кілька компонентів довіри. Цей підрозділ сімейства довіри містить опис наявних компонентів і пояснення їх характерних ознак. Його основна мета полягає у вказівці відмінностей між компонентами при ухваленні рішення про те, що сімейство є необхідною або корисною частиною вимог довіри для ПЗ / ЗБ.

У родинах довіри, входить більш як один компонент, виконано ранжування компонентів і приведено його обгрунтування. Це обгрунтування сформульовано в термінах області охоплення, глибини і / або строгості.

3.1.2.3 Зауваження по застосуванню

Необов'язковий підрозділ сімейства довіри "Зауваження щодо застосування" містить додаткову інформацію про сімейства. Ця інформація призначена безпосередньо для користувачів сімейства довіри (наприклад, для розробників ПЗ і ЗБ, проектувальників ОО, оцінювачів). Подання інформації неформальне і включає в себе, наприклад, попередження про обмеження використання або областях, що вимагають особливої уваги.

3.1.3 Структура компонента

На Рисунку 3.1.3 представлена структура компонента довіри.

Рисунок 3.1.3 Структура компонента довіри

Зв'язки між компонентами всередині сімейства показано жирними лініями. Для частини вимог, які є новими, розширеними або модифікованими в порівнянні з вимогами попереднього по ієрархії компонента, застосований напівжирний шрифт.

3.1.3.1 Цілі

Необов'язковий підрозділ "Цілі" компонента довіри містить конкретні цілі для даного компонента. Для компонентів довіри, які мають цей підрозділ, він включає в себе конкретне призначення даного компонента і більш докладне роз'яснення цілей.

3.1.3.2 Зауваження по застосуванню

Необов'язковий підрозділ компонента довіри "Зауваження по застосуванню", при його наявності, містить додаткову інформацію для полегшення використання компонента.

3.1.3.3 Елементи довіри

Кожен компонент довіри містить набір елементів довіри. Елемент довіри є вимогою безпеки, при подальшому поділі який не змінює значущий результат оцінки. Він є найменшою вимогою безпеки.

Кожен елемент довіри належить до одного з трьох типів:

a)Елементи дій розробника, що визначають дії, які повинні виконуватися розробником. Цей набір дій далі уточнюється доказовим матеріалом, які згадуються в подальшому наборі елементів. Вимоги до дій розробника позначені літерою "D" після номеру елементу.

b)Елементи змісту і надання доказів, що визначають необхідні свідчення і відображається в них інформацію. Вимоги до змісту та поданням свідчень позначені літерою "C" після номеру елементу.

c)Елементи дій оцінювача, що визначають дії, які повинні виконуватися оцінювачем. Цей набір дій безпосередньо включає в себе

підтвердження того, що вимоги, визначені елементами змісту і надання доказів, виконані, а також явні дії і аналіз, які повинні виконуватися на додаток до вже проведених розробником. Повинні також виконуватися не зазначені явно дії оцінювача, необхідні внаслідок елементів дій розробника, але не охоплені в вимогах до змісту і поданням свідчень. Вимоги до дій оцінювача позначаються літерою "Е" після номеру елементу.

Дії розробника, зміст і представлення свідчень визначають вимоги довіри, які пред'являються до розробника при демонстрації довіри до того, що ОО задовольняє ФТБ з ПЗ або ЗБ. [7]

Дії оцінювача визначають його відповідальність за двома аспектами оцінки. Перший аспект полягає в перевірці правильності ПЗ / ЗБ відповідно до вимог класів АРЄ "Оцінка профілю захисту" і ASE "Оцінка завдання з безпеки". Другий аспект полягає в верифікації відповідності ОО його функціональним вимогам і вимогам довіри. Демонструючи, що ПЗ / ЗБ правильні і їх умови виконуються ОО, оцінювач може надати підставу для впевненості в тому, що ОО буде відповідати поставленим цілям безпеки.

Елементи дій розробника, елементи змісту і надання доказів та елементи явних дій оцінювача визначають рівень його зусиль, які повинні бути включені при верифікації тверджень про безпеку, сформульованих в ЗБ конкретного ОО.

Кожен елемент представляє собою обов'язкову для виконання вимогу. Формулювання цих вимог повинні бути чіткими, короткими і однозначними. Тому у вимогах відсутні складові пропозиції. Кожне вимога викладена як окремий елемент.

3.1.4 Класифікація компонентів

В ISO / IEC 15408-3 містяться класи сімейств і компонентів, які згруповані на основі, пов'язаної з довірою. На початку кожного класу подано діаграму, на якій вказуються сімейства в класі і компоненти в кожному сімействі.

На рисунку 3.1.4 показаний клас, що містить одне сімейство. Сімейство містить три компонента, які є лінійно ієрархічними (тобто компонент 2 містить більш високі вимоги, ніж компонент 1, до конкретних дій, які наводяться свідченнями або строгості дій і / або свідоцтв). Всі сімейства довіри в ISO / IEC 15408-3 - лінійно ієрархічні, хоча лінійність необов'язкова для родин довіри, які можуть бути додані в подальшому.

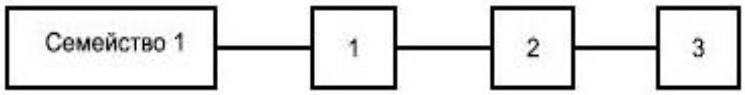

Рисунок 3.1.4 Зразок декомпозиції класу

3.1.5 Структура Орд

Рис 3.1.5 ілюструє Орд і їх структуру, визначену в ISO / IEC 15408-3. Компоненти довіри, зміст яких показано на малюнку, включені в Орд за допомогою посилань на компоненти, наведені в ISO / IEC 15408-3.

Кожному Орд присвоєно унікальне ім'я. Ім'я являє описову інформацію про призначення Орд.

Представлена також унікальна коротка форма імені Орд. Вона є основним засобом посилання на Орд.

Рисунок 3.1.5 Структура Орд

3.1.6 Зауваження щодо застосування

Необов'язковий підрозділ Орд "Зауваження щодо застосування" містить інформацію, що представляє інтерес для користувачів Орд (наприклад, для розробників ПЗ і ЗБ, проектувальників ОО, які планують використання цього Орд, оцінювачів). Подана неформально і включає в

себе, наприклад, попередження про обмеження використання або областях, що вимагають особливої уваги.

3.1.7 Компоненти довіри

Для кожного Орд обраний набір компонентів вимог довіри.

Більш високий рівень довіри, ніж надається конкретним Орд, може бути досягнуто:

a)включенням додаткових компонентів вимог довіри з інших сімейств довіри або

b)заміною компонента вимог довіри ієрархічними компонентом з цього ж сімейства вимог довіри.

3.1.8 Взаємозв'язок між вимогами і рівнями довіри

Рисунок 3.1.8 ілюструє взаємозв'язок між вимогами довіри і рівнями довіри, визначеними в ISO / IEC 15408-3. Компоненти довіри складаються з елементів, але на останні окремо не можуть посилатися оціночні рівні довіри. Стрілка на малюнку відображає посилання в Орд на компонент вимог довіри всередині класу, в якому він визначений.

3.1.9 Структура СПД

Структура СПД аналогічна структурі Орд. Ключове відмінність двох структур полягає в типі ОО, до яких вони застосовуються; Орд застосовується до ОО-компонентів, а СПД- до всього складеному ОО в цілому.

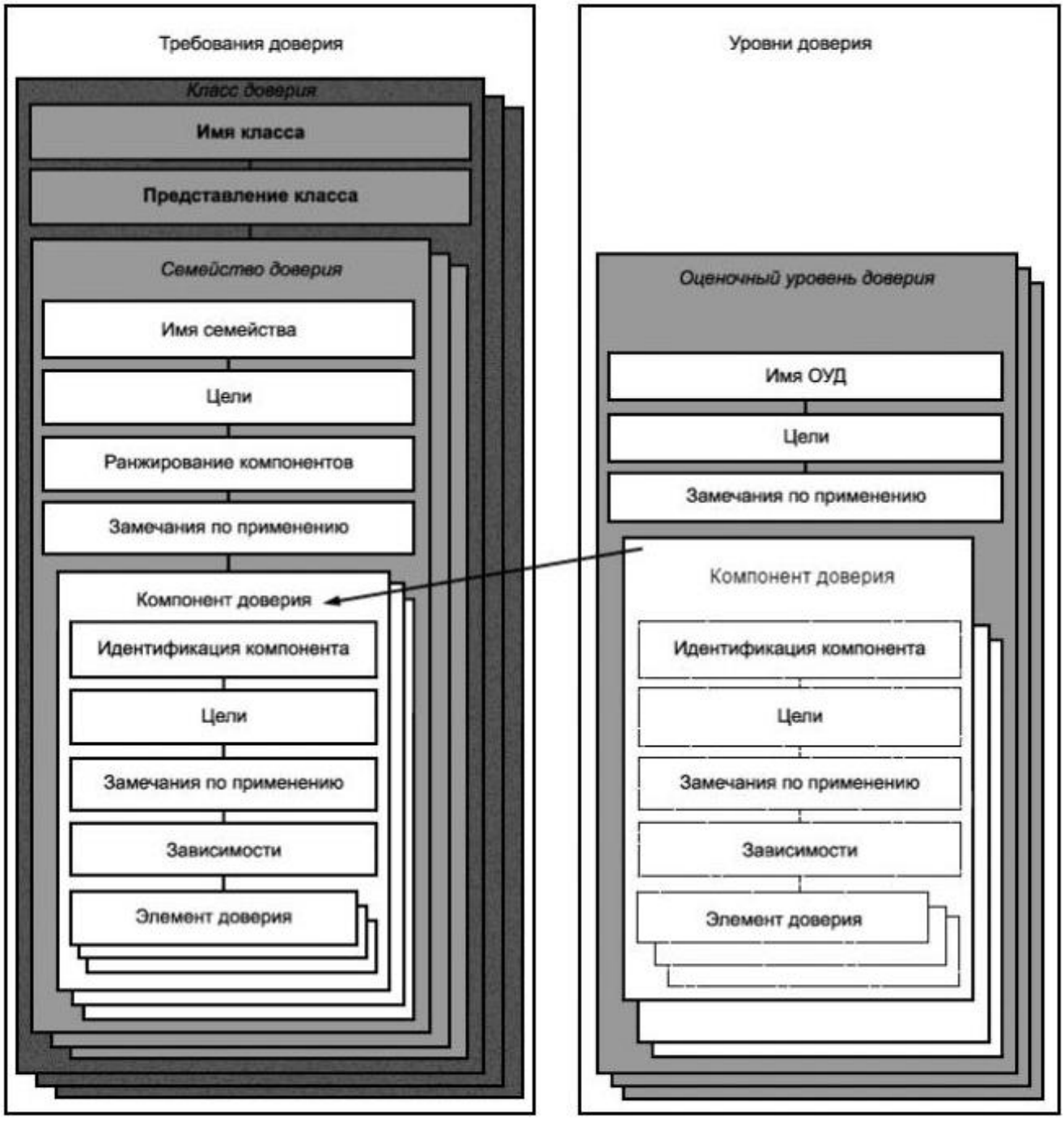

Рисунок 3.1.8 Взаємозв'язок вимог і рівня довіри

На рисунку 3.1.9 показана структура СПД, представлена в ISO / IEC 15408-3. Слід зауважити, що хоч на малюнку показано вміст компонентів довіри, передбачається, що ця інформація буде включатися в СПД за допомогою посилання на компоненти ISO / IEC 15408.

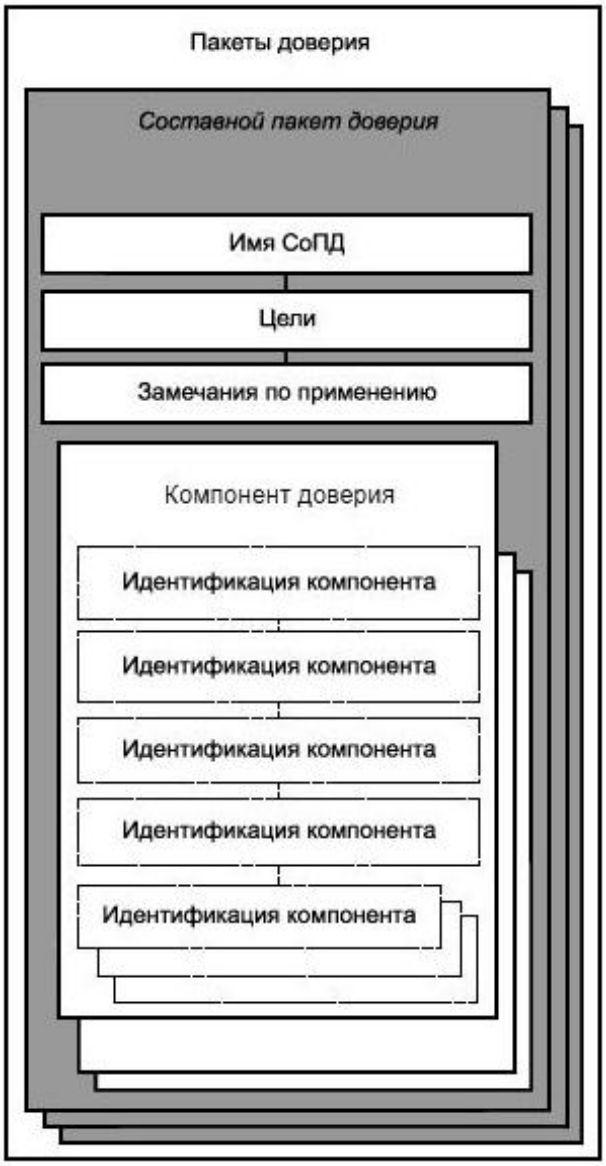

Рисунок 3.1.9 Структура СПД

3.1.10 Ім'я СПД

Кожному СПД присвоєно унікальне ім'я. Ім'я надає описову інформацію, що характеризує призначення СПД.

Представлена також унікальна коротка форма імені СПД. Вона є основним засобом посилання на СПД.

3.1.11 Компоненти довіри

Набір компонентів довіри встановлений для кожного СПД.

Деякі залежності визначають дії, що виконуються в процесі оцінки конкретного залежного компонента, на які спираються дії по оцінці складеного ОО. У разі, якщо явно не визначено наявність залежності від дій по оцінці залежного компонента, залежність відноситься до іншого дії по оцінці складеного ОО. [7]

Більш високий рівень довіри в порівнянні з конкретним СПДдосягається шляхом:

a)додавання компонентів довіри з інших сімейств довіри;

b)заміни компонента довіри на більш високий за ієрархією компонент з того ж сімейства довіри.

Компоненти класу АСО "Композиція", включені в СПД, не слід використовувати в якості посилення при оцінці ОО-компонента, оскільки це не забезпечить значного довіри до цього ОО-компоненту

3.1.12 Взаємозв'язок між вимогами довіри і складовими пакетами довіри

На рисунку 3.1.12 показано взаємозв'язок між вимогами довіри до безпеки і складовими пакетами довіри, визначеними в ISO / IEC 15408. Компоненти довіри складаються з елементів, але на останні не можуть окремо посилатися на пакети вимог довіри. Стрілка на малюнку відображає посилання від СПД на компонент довіри всередині класу, в якому він визначений.

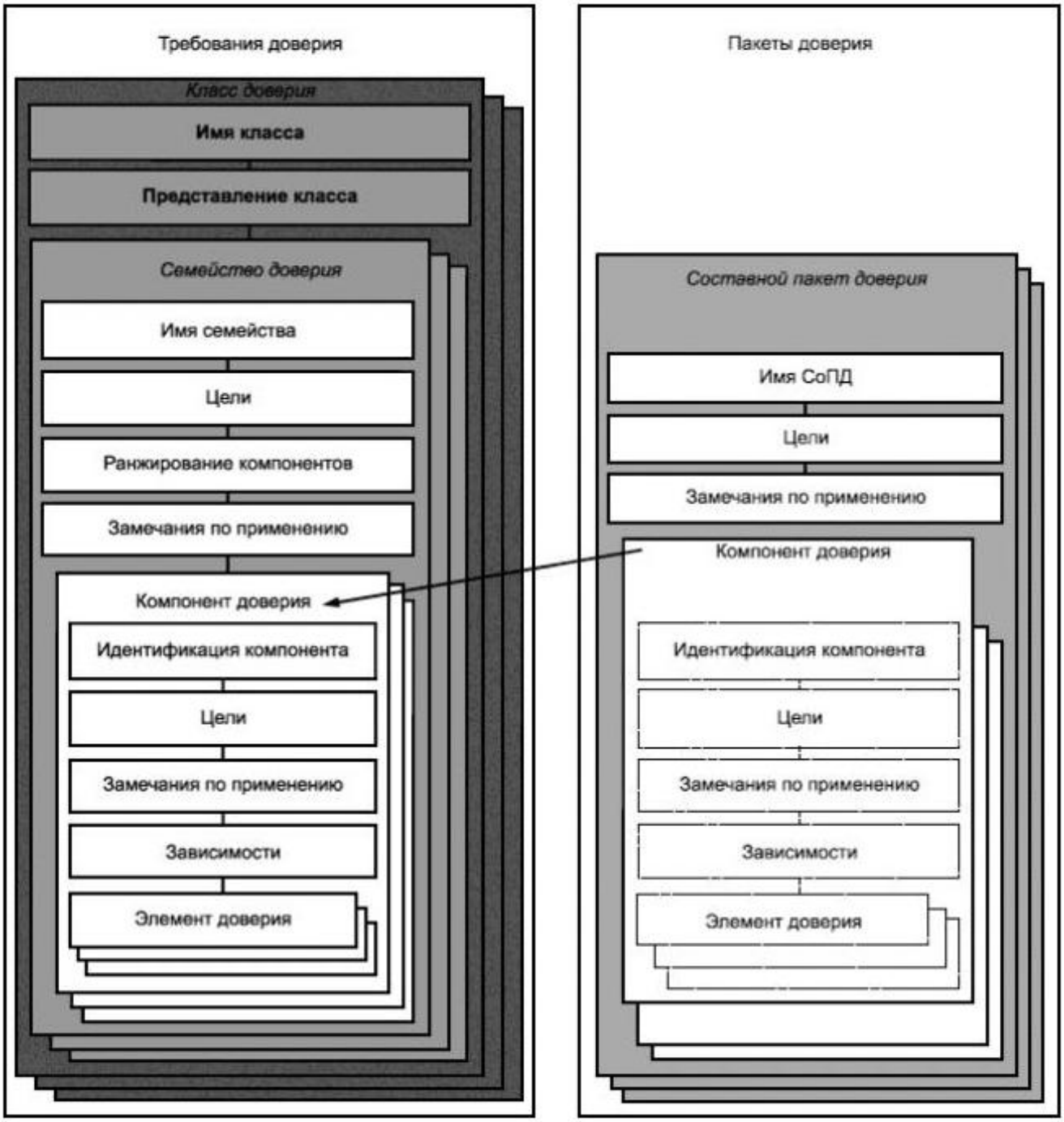

Рисунок 3.1.12 Взаємозв'язок між вимогами довіри і складовими пакетами довіри

3.2 Оціночні рівні довіри

Оціночні рівні довіри (Орд) утворюють зростаючу шкалу, яка дозволяє спів-віднести отриманий рівень довіри з вартістю і можливістю досягнення цього ступеня довіри. У підході ISO / IEC 15408 визначаються окремі поняття для довіри до ОО після завершення оцінки і по підтримці довіри під час експлуатації ОО.

Важливо звернути увагу, що не всі сімейства і компоненти ISO / IEC 15408 включені в оціночні рівні довіри. Це не означає, що вони не забезпечують зазначену і очікувану довіру. Навпаки, очікується, що ці сімейства і їх компоненти будуть використовуватися для посилення Орд в тих ПЗ і ЗБ, для яких вони корисні.

У таблиці 1 представлено зведений опис Орд. Стовпці таблиці представляють ієрархічно упорядкований набір Орд, а рядки - сімейства довіри. Кожен номер в утвореної ними матриці ідентифікує конкретний компонент довіри, застосовуваний в даному випадку.

Кожен наступний Орд представляє більш високу довіру, ніж будь-який з попередніх. Збільшення довіри від попереднього Орд до подальшого досягається заміною будь-якого компонента довіри ієрархічними компонентом з того ж сімейства довіри (тобто збільшенням строгості, області охоплення або глибини оцінки) і додаванням компонентів з інших сімейств довіри (тобто додаванням нових вимог).

Кожен Орд включає в себе не більше одного компонента кожного сімейства довіри, при цьому враховуються всі залежності кожного компонента довіри.

Хоча в ISO / IEC 15408-3 визначені саме Орд, можна представляти інші комбінації компонентів довіри. Спеціально введене поняття "посилення" ("augmentation") допускає додавання (з сімейств довіри, які

не включені в Орд) або заміну компонентів довіри в Орд (іншими, ієрархічними компонентами з того ж самого сімейства довіри). З конструкцій встановлення довіри, визначених у ISO / IEC 15408, тільки Орд можуть бути посилені. Поняття "Орд за винятком будь-якого становить його компонент довіри" не визнана в ISO / IEC 15408 як допустимий.

Таблиця 3.1 – Опис Орд

Класс доверия	Семейство доверия	Компоненты доверия из оценочного уровня доверия						
		ОУД1	ОУД2	ОУД3	ОУД4	ОУД5	ОУД6	ОУД7
Разработка	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Руководства	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Поддержка жизненного цикла	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Оценка задания по безопасности	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Тестирование	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Оценка уязвимостей	AVA_VAN	1	2	2	3	4	5	5

3.2.1 Оціночний рівень довіри 1 (ОРД1)

3.2.1.1 Цілі

Передбачає функціональне тестування.

ОРД1 застосуємо, коли потрібна деяка впевненість у правильному функціонуванні ОО, а загрози безпеки не розглядають як серйозні. Він

буде корисний там, де потрібно незалежно отриману довіру твердженням, що було приділено належну увагу захисту інформації з низьким рівнем необхідності.

Для ОРД1 потрібно тільки ЗБ зі скороченим змістом. Можна не визначати функціональні вимоги шляхом вивчення загроз, ПБОр і припущень про цілі безпеки; досить просто викласти, яким функціональним вимогам повинен відповідати ОО. [7]

ОРД1 забезпечує оцінку ОО в тому вигляді, в якому він доступний споживачеві, шляхом незалежного тестування на відповідність специфікації і експертизи поданої документації посібників. Передбачається, що оцінка по ОРД1 може успішно проводитися без допомоги розробника ОО і з мінімальними витратами.

При оцінці на цьому рівні слід надати свідоцтво, що ОО функціонує відповідно до його документацією.

3.2.1.2 Компоненти довіри

ОРД1 надає базовий рівень довіри за допомогою ЗБ зі скороченим змістом і аналіз ФВБ в цьому ЗБ з використанням функціональної специфікації, специфікації інтерфейсів і посібників для розуміння режиму безпеки.

Аналіз підтриманий пошуком потенційних вразливостей (шляхом вивчення загальнодоступної інформації) з проведенням незалежного тестування (функціонального і тестування проникнення) ФБО.

Також ОРД1 забезпечує довіру завдяки унікальній ідентифікації ОО і документації по оцінці.

Таблиця 3.2 - ОРД1

клас довіри	компоненти довіри
ADV: Розробка	ADV_FSP.1 Базова функціональна специфікація
AGD: Керівництва	AGD_OPE.1 Керівництво користувача по експлуатації
	AGD_PRE.1 Підготовчі процедури
ALC: Підтримка життєвого циклу	ALC_CMC.1 Маркування ОО
	ALC_CMS.1 Охоплення КК об'єкта оцінки
ASE: Оцінка завдання з безпеки	ASE_CCL.1 Твердження про відповідність
	ASE_ECD.1 Визначення розширених компонентів
	ASE_INT.1 Введення ЗБ
	ASE_OBJ.1 Цілі безпеки для середовища функціонування
	ASE_REQ.1 Встановлені вимоги безпеки
	ASE_TSS.1 Коротка специфікація ОО
ATE: Тестування	ATE_IND.1 Незалежне тестування на відповідність
AVA: Оцінка вразливостей	AVA_VAN.1 Огляд вразливостей

Цей Орд забезпечує значуще збільшення довіри в порівнянні з продуктом ІТ, що не була піддана оцінці.

3.2.2 Оціночний рівень довіри 2 (ОРД2)

3.2.2.1 Цілі

Передбачає структурне тестування.

ОРД2 містить вимогу співпраці з розробником для отримання інформації про проект та результати тестування, але при цьому не слід вимагати від розробника зусиль, що перевищують звичайну комерційну практику. Отже, не потрібно істотного збільшення вартості або витрат часу.

Тому ОРД2 застосуємо, коли розробникам або користувачам потрібно незалежно підтвердити рівень довіри від невисокого до помірного при відсутності доступу до повної документації по розробці. Така ситуація може виникати при забезпеченні безпеки розроблених раніше (успадкованих) систем або при обмеженій доступності розробника.

3.2.2.2 Компоненти довіри

ОРД2 забезпечує довіру за допомогою ЗБ з повним змістом і за допомогою аналізу виконання ФВБ з даного ЗБ з використанням функціональної специфікації, специфікації інтерфейсів, посібників, а також базового опису архітектури ОО для розуміння режиму безпеки.

Аналіз підтриманий незалежним тестуванням ФБО, свідченням розробника про тестування, заснованому на функціональній специфікації, вибірковим незалежним підтвердженням результатів тестування розробником, і аналізом вразливостей (заснованим на функціональній специфікації, проект ОО, описі архітектури системи безпеки і документації посібників), що демонструє протистояння спробам проникнення порушників, володіє Базовим потенціалом нападу. [7]

Таблиця 3.3 - ОРД2

клас довіри	компоненти довіри
ADV: Розробка	ADV_ARC.1 Опис архітектури безпеки
	ADV_FSP.2 Деталізація питань безпеки в функціональної специфікації
	ADV_TDS.1 Базовий проект
AGD: Керівництва	AGD_OPE.1 Керівництво користувача по експлуатації
	AGD_PRE.1 Підготовчі процедури
ALC:Підтримка життєвого циклу	ALC_CMC.2 Використання системи КК
	ALC_CMS.2 Охоплення КК частин ОО
	ALC_DEL.1 Процедури поставки
ASE:Оцінка завдання з безпеки	ASE_CCL.1 Твердження про відповідність
	ASE_ECD.1 Визначення розширених компонентів
	ASE_INT.1 Введення ЗБ
	ASE_OBJ.2 Цілі безпеки
	ASE_REQ.2 Похідні вимоги безпеки
	ASE_SPD.1 Визначення проблеми безпеки
	ASE_TSS.1 Коротка специфікація ОО
ATE: Тестування	ATE_COV.1 Свідоцтво покриття
	ATE_FUN.1 Функціональне тестування
	ATE_IND.2 Вибіркове незалежне тестування
AVA:Оцінка вразливостей	AVA_VAN.2 Аналіз вразливостей

ОРД2 також забезпечує довіру за допомогою використання системи управління конфігурацією ОО і свідоцтва безпечних процедур поставки.

ОРД2 представляє значне збільшення довіри в порівнянні з ОРД1, вимагаючи тестування ОО і аналіз вразливостей розробником (крім вивчення загальнодоступних джерел інформації), а також незалежне тестування, засноване на більш деталізованих специфікаціях ОО.

3.2.3 Оціночний рівень довіри 3 (ОРД3)

3.2.3.1 Цілі

Що передбачає методичне тестування і перевірку.

ОРД3 дозволяє сумлінному розробнику досягти максимальної довіри шляхом застосування належного проектування безпеки на стадії розробки проекту без внесення суттєвих змін до існуючої практики якісної розробки.

ОРД3 застосуємо, коли розробникам або користувачам потрібно незалежно підтверджений помірний рівень довіри на основі всебічного дослідження ОО і процесу його розробки без істотних витрат на зміну технології проектування.

3.2.3.2 Компоненти довіри

ОРД3 забезпечує довіру за допомогою ЗБ з повним змістом і за допомогою аналізу виконання ФТБ з даного ЗБ з використанням функціональної специфікації, специфікації інтерфейсів, посібників і архітектурного опису проекту ОО для розуміння режиму безпеки.

Таблиця 3.4 - ОРД3

клас довіри	компоненти довіри
ADV: Розробка	ADV_ARC.1 Опис архітектури безпеки
	ADV_FSP.3 Функціональна специфікація з повною анотацією
	ADV_TDS.2 Архітектурний проект
AGD: Керівництва	AGD_OPE.1 Керівництво користувача по експлуатації
	AGD_PRE.1 Підготовчі процедури
ALC:Підтримка життєвого циклу	ALC_CMC.3 Засоби управління авторизацією
	ALC_CMS.3 Охоплення КК уявлення реалізації
	ALC_DEL.1 Процедури поставки
	ALC_DVS.1 Ідентифікація заходів безпеки
	ALC_LCD.1 Певна розробником модель життєвого циклу
ASE: Оцінка завдання з безпеки	ASE_CCL.1 Твердження про відповідність
	ASE_ECD.1 Визначення розширених компонентів
	ASE_INT.1 Введення ЗБ
	ASE_OBJ.2 Цілі безпеки
	ASE_REQ.2 Похідні вимоги безпеки
	ASE_SPD.1 Визначення проблеми безпеки
	ASE_TSS.1 Коротка специфікація ОО

Аналіз підтриманий незалежним тестуванням ФБО, свідченням розробника про тестування, заснованому на функціональної специфікації і проект ОО, вибірковим незалежним підтвердженням результатів тестування розробником і аналізом вразливостей (заснованим на представлених свідченнях по функціональній специфікації, проекту ОО, опису архітектури безпеки і посібникам), що демонструє протистояння спробам проникнення порушників, які мають Базовий потенціал нападу.

ОРД3 також забезпечує довіру за допомогою використання заходів управління середовищем розробки, управління конфігурацією ОО і свідоцтва безпечних процедур поставки.

ОРД3 представляє значуще збільшення довіри в порівнянні з ОРД2, вимагаючи більш повного покриття тестуванням функціональних можливостей і механізмів безпеки і процедур безпеки, що дає деяку впевненість в тому, що в ОО не будуть внесені спотворення під час розробки.

3.2.4 Оціночний рівень довіри 4 (ОРД4)

3.2.4.1 Цілі

Передбачає методичне проектування, тестування і поглиблену перевірку.

ОРД4 дозволяє розробнику досягти максимальної довіри шляхом застосування належного проектування безпеки, заснованого на хороших комерційних практиках розробки, які, навіть будучи строгими, не вимагають глибоких професійних знань, навичок та інших ресурсів. ОРД4 - найвищий рівень, на який, ймовірно, економічно доцільно орієнтуватися при оцінці вже існуючих продуктів.

Тому ОРД4 застосуємо, коли розробникам або користувачам потрібно незалежно підтверджений рівень довіри від помірного до високого в ОО загального призначення і є готовність нести додаткові, пов'язані із забезпеченням безпеки, виробничі витрати.

3.2.4.2 Компоненти довіри

ОРД4 забезпечує довіру за допомогою ЗБ з повним змістом і за допомогою аналізу виконання ФВБ з даного ЗБ з використанням функціональної специфікації, повної специфікації інтерфейсів, посібників, опису базового модульного проекту ОО, а також підмножини реалізації для розуміння режиму безпеки.

Аналіз підтриманий незалежним тестуванням ФБО, свідченням розробника про тестування, заснованому на функціональної специфікації і проект ОО, вибірковим незалежним підтвердженням результатів тестування розробником і аналізом вразливостей (заснованим на представлених свідченнях по функціональній специфікації, проекту ОО, поданням реалізації, опису архітектури безпеки і посібникам), що демонструє протистояння спробам проникнення порушників, які мають посиленим Базовий потенціал нападу.

ОРД4 також забезпечує довіру за допомогою використання заходів управління середовищем розробки і додаткового управління конфігурацією ОО, включаючи автоматизацію, і свідоцтва безпечних процедур поставки.

ОРД4 представляє значуще збільшення довіри в порівнянні з ОРД3, вимагаючи більш детальний опис проекту, представлення реалізації для всіх ФБО і поліпшені механізми і / або процедури, що дають впевненість у тому, що в ОО не буде внесено спотворення під час розробки.

Таблиця 3.5- ОРД4

клас довіри	компоненти довіри
ADV: Розробка	ADV_ARC.1 Опис архітектури безпеки
	ADV_FSP.4Повна функціональна специфікація
	ADV_IMP.1 Подання реалізації ФБО
	ADV_TDS.3 Базовий модульний проект
AGD: Керівництва	AGD_OPE.1 Керівництво користувача по експлуатації
	AGD_PRE.1 Підготовчі процедури
ALC:Підтримка життєвого циклу	ALC_CMC.4 Підтримка виробництва, процедури приймання та автоматизації
	ALC_CMS.4 Охоплення КК відстеження проблем
	ALC_DEL.1 Процедури поставки
	ALC_DVS.1 Ідентифікація заходів безпеки
	ALC_LCD.1 Певна розробником модель життєвого циклу
	ALC_TAT.1 Повністю певні інструментальні засоби розробки
ASE: Оцінка завдання з безпеки	ASE_CCL.1 Твердження про відповідність
	ASE_ECD.1 Визначення розширених компонентів
	ASE_INT.1 Введення ЗБ
	ASE_OBJ.2 Цілі безпеки
	ASE_REQ.2 Похідні вимоги безпеки

3.2.5 Оціночний рівень довіри 5 (ОРД5)

3.2.5.1 Цілі

Передбачає напів-формального проектування і тестування.

ОРД5 дозволяє розробнику досягти максимальної довіри шляхом проектування безпеки, заснованого на суворої комерційній практиці розробки, підтриманого помірним застосуванням спеціалізованих методів проектування безпеки. Такі ОО будуть, ймовірно, проектуватися і розроблятися з наміром досягти ОРД5. Швидше за все, додаткові витрати, супутні вимогам ОРД5 в частині строгості розробки без застосування спеціалізованих методів розробки, які не будуть великими.

Тому ОРД5 застосуємо, коли розробникам або користувачам потрібно незалежно одержуваний високий рівень довіри для запланованої розробки із суворим підходом до розробки, які не потребують зайвих витрат на застосування вузько спеціалізованих методів проектування безпеки.

3.2.5.2 Компоненти довіри

ОРД5 забезпечує довіру за допомогою ЗБ з повним змістом і за допомогою аналізу виконання ФВБ з даного ЗБ з використанням функціональної специфікації, повної специфікації інтерфейсів, посібників, опису проекту ОО, а також всієї його реалізації для розуміння режиму безпеки. Крім цього, також потрібно модульне проектування ФБО.

Аналіз підтриманий незалежним тестуванням ФБО, свідченням розробника про тестування, заснованому на функціональної специфікації, проект ОО, вибірковим незалежним підтвердженням результатів тестування розробником і незалежним аналізом вразливостей, що

демонструє протистояння спробам проникнення порушників з помірним потенціалом нападу.

Таблиця 3.6 - ОРД5

клас довіри	компоненти довіри
ADV: Розробка	ADV_ARC.1 Опис архітектури безпеки
	ADV_FSP.5 Повна напівформального специфікація з додатковою інформацією про помилки
	ADV_IMP.1 Подання реалізації ФБО
	ADV_INT.2 Повністю певна внутрішня структура
	ADV_TDS.4 напів-формально модульний проект
AGD: Керівництва	AGD_OPE.1 Керівництво користувача по експлуатації
	AGD_PRE.1 Підготовчі процедури
ALC: Підтримка життєвого циклу	ALC_CMC.4 Підтримка виробництва, процедури приймання та автоматизації
	ALC_CMS.5 Охоплення КК інструментальних засобів розробки
	ALC_DEL.1 Процедури поставки
	ALC_DVS.1 Ідентифікація заходів безпеки
	ALC_LCD.1 Певна розробником модель життєвого циклу
	ALC_TAT.2 Відповідність стандартам реалізації
ASE: Оцінка завдання з безпеки	ASE_CCL.1 Твердження про відповідність

Продовження таблиці 3.6 - ОРД5

	ASE_ECD.1 Визначення розширених компонентів
	ASE_INT.1 Введення ЗБ
	ASE_OBJ.2 Цілі безпеки
	ASE_REQ.2 Похідні вимоги безпеки
	ASE_SPD.1 Визначення проблеми безпеки
	ASE_TSS.1 Коротка специфікація ОО
ATE: Тестування	ATE_COV.2 Аналіз покриття
	ATE_DPT.3 Тестування: модульний проект
	ATE_FUN.1 Функціональне тестування
	ATE_IND.2 Вибіркове незалежне тестування
AVA:Оцінка вразливостей	AVA_VAN.4 Методичний аналіз вразливостей

ОРД5 також забезпечує довіру за допомогою використання контролю середовища розробки та всебічного управління конфігурацією ОО, включаючи автоматизацію, і свідоцтва безпечних процедур поставки.

ОРД5 представляє значне збільшення довіри в порівнянні з ОРД4, вимагаючи напів-формального опис проекту, більш структуровану архітектуру і поліпшені механізми і процедури, що дають впевненість у тому, що в ОО не будуть внесені спотворення під час розробки .

3.2.6 Оціночний рівень довіри 6 (ОРД6)

3.2.6.1 Цілі

Передбачає напів-формального верифікацію і тестування проекту.

ОРД6 дозволяє розробникам досягти високої довіри шляхом застосування методів проектування безпеки в строго контрольованому середовищі розробки з метою отримання високоякісного ОО для захисту високо оцінюваних активів від значних ризиків.

3.2.6.2 Компоненти довіри

ОРД6 забезпечує довіру за допомогою ЗБ з повним змістом і за допомогою аналізу виконання ФВБ з даного ЗБ з використанням функціональної специфікації, повної специфікації інтерфейсів, посібників, проекту ОО, а також уявлення реалізації для розуміння режиму безпеки. Довіра додатково досягається застосуванням формальної моделі обраної політики безпеки ОО і напів-формального уявлення функціональної специфікації, а також проекту ОО. Крім цього, також потрібно модульний і ієрархічний проект ФБО.

Таблиця 3.7 - ОРД6

клас довіри	компоненти довіри
ADV: Розробка	ADV_ARC.1 Опис архітектури безпеки
	ADV_FSP.5 Повна напівформального функціональна специфікація з додатковою інформацією про помилки
	ADV_IMP.2 Повний простежування уявлення реалізації ФБО

Продовження таблиці 3.7 - ОРД6

	ADV_INT.3 Мінімальна складність внутрішньої структури системи
	ADV_SPM.1 Формальна модель політики безпеки ОО
	ADV_TDS.5 Повний напівформального модульний проект
AGD: Керівництва	AGD_OPE.1 Керівництво користувача по експлуатації
	AGD_PRE.1 Підготовчі процедури
ALC:Підтримка життєвого циклу	ALC_CMC.5 Розширена підтримка
	ALC_CMS.5 Охоплення КК інструментальних засобів розробки
	ALC_DEL.1 Процедури поставки
	ALC_DVS.2 Достатність заходів безпеки
	ALC_LCD.1 Певна розробником модель життєвого циклу
	ALC_TAT.3 Відповідність всіх частин ОО стандартам реалізації
ASE:Оцінка завдання з безпеки	ASE_CCL.1 Твердження про відповідність
	ASE_ECD.1 Визначення розширених компонентів
	ASE_INT.1 Введення ЗБ
	ASE_OBJ.2 Цілі безпеки
	ASE_REQ.2 Похідні вимоги безпеки

Продовження таблиці 3.7 - ОРД6

	ASE_SPD.1 Визначення проблеми безпеки
	ASE_TSS.1 Коротка специфікація ОО
ATE: Тестування	ATE_COV.3 Строгий аналіз покриття
	ATE_DPT.3 Тестування: модульний проект
	ATE_FUN.2 Впорядковане функціональне тестування
	ATE_IND.3 Вибіркове незалежне тестування
AVA:Оцінка вразливостей	AVA_VAN.5 Посилений методичний аналіз вразливостей

3.2.7 Оціночний рівень довіри 7 (ОРД7)

3.2.7.1 Цілі

Передбачає формальну верифікацію проекту і тестування.

ОРД7 застосуємо при розробці безпечних ОО для використання в умовах надзвичайно високого ризику та там, де висока цінність активів виправдовує підвищені витрати. Практичне застосування ОРД7 в даний час обмежений ОО, які строго орієнтовані на реалізацію функціональних можливостей безпеки і для яких можливий всебічний формальний аналіз.

3.2.7.2 Компоненти довіри

ОРД7 забезпечує довіру за допомогою ЗБ з повним змістом і за допомогою аналізу виконання ФВБ з даного ЗБ з використанням функціональної специфікації, повної специфікації інтерфейсів, посібників, проекту ОО, а також структурного представлення реалізації. Довіра

додатково досягається застосуванням формальної моделі обраної політики безпеки ОО, напів-формального уявлення функціональної специфікації та проекту ОО для розуміння режиму безпеки. Крім цього, потрібно також модульний, ієрархічний (за рівнями) і простий проект ФБО.

Таблиця 3.8 - ОРД7

клас довіри	компоненти довіри
ADV: Розробка	ADV_ARC.1 Опис архітектури безпеки
	ADV_FSP.6 Повна напівформального функціональна специфікація з додатковою формальної специфікації
	ADV_IMP.2 Повний простежування уявлення реалізації ФБО
	ADV_INT.3 Мінімальна складність внутрішньої структури системи
	ADV_SPM.1 Формальна модель політики безпеки ОО
	ADV_TDS.6 Повний напівформального модульний проект з формальним поданням проекту верхнього рівня
AGD: Керівництва	AGD_OPE.1 Керівництво користувача по експлуатації
	AGD_PRE.1 Підготовчі процедури
ALC: Підтримка життєвого циклу	ALC_CMC.5 Розширена підтримка

Продовження таблиці 3.8 - ОРД7

	ALC_CMS.5 Охоплення КК інструментальних засобів розробки
	ALC_DEL.1 Процедури поставки
	ALC_DVS.2 Достатність заходів безпеки
	ALC_LCD.2 Вимірна модель життєвого циклу
	ALC_TAT.3 Відповідність всіх частин ОО стандартам реалізації
ASE: Оцінка завдання з безпеки	ASE_CCL.1 Твердження про відповідність
	ASE_ECD.1 Визначення розширених компонентів
	ASE_INT.1 Введення ЗБ
	ASE_OBJ.2 Цілі безпеки
	ASE_REQ.2 Похідні вимоги безпеки
	ASE_SPD.1 Визначення проблеми безпеки
	ASE_TSS.1 Коротка специфікація ОО
ATE: Тестування	ATE_COV.3 Строгий аналіз покриття
	ATE_DPT.4 Тестування: уявлення реалізації
	ATE_FUN.2 Впорядковане функціональне тестування
	ATE_IND.3 Повний незалежне тестування

Аналіз підтриманий незалежним тестуванням ФБО, свідченням розробника про тестування, заснованому на функціональної специфікації, проект ОО і поданні реалізації, повним незалежним підтвердженням результатів тестування розробником і незалежним аналізом вразливостей,

що демонструє протистояння спробам проникнення порушників з Високим потенціалом нападу. [7]

ОРД7 також забезпечує довіру за допомогою використання структурованого процесу розробки, засобів контролю середовища розробки та всебічного управління конфігурацією ОО, включаючи повну автоматизацію, і свідоцтва безпечних процедур поставки.

ОРД7 представляє значуще збільшення довіри в порівнянні з ОРД6, вимагаючи більш всебічний аналіз, що використовує формальні уявлення і формальну відповідність, а також всебічне тестування.

3.3 Аналіз складових пакетів довіри

Складові пакети довіри (СПД) утворюють зростаючу шкалу, яка дозволяє спів-віднести рівень отриманого довіри з витратами і можливістю досягнення цього ступеня довіри для складових ОО.

Важливо відзначити, що лише невелика частина родин і компонентів довіри з ISO / IEC 15408-3 включена в складові пакети довіри. Це пов'язано з тим, що вони ґрунтуються на результатах оцінки раніше оцінених сутностей (базових компонентів і залежних компонентів) і в зв'язку з цим не можна говорити, що вони не забезпечують значну і необхідну довіру.

3.3.1 Огляд складових пакетів довіри (СПД)

СПД застосовуються до складових ОО, які містять компоненти, які пройшли (або проходять) оцінку як ОО-компоненти. Окремі компоненти повинні бути сертифіковані по Орд або іншому пакету довіри, вказаною в ЗБ. Передбачається, що базовий рівень довіри для складеного ОО буде отриманий за допомогою застосування ОРД1, який може бути досягнутий

з використанням загальнодоступної інформації про компоненти (ОРД1 може застосовуватися як до окремих ОО-компонентів, так і до складових ОО). СПД представляють альтернативний підхід до отримання більш високих рівнів довіри для складеного ОО в порівнянні з застосуванням Орд вище ОРД1.

Хоча залежний компонент може бути оцінений з використанням раніше оцінених і сертифікованих базових компонентів для задоволення вимог, що пред'являються до IT-платформи в середовищі функціонування, це не забезпечує будь-якого формального рівня довіри до взаємодії компонентів або по відношенню до обліку можливої появи вразливостей при об'єднанні компонентів . Складові пакети довіри враховують такі взаємодії і на більш високих рівнях довіри забезпечують, що інтерфейси між компонентами є предметом тестування. Також виконується аналіз вразливостей складеного ОО з метою врахування можливої появи вразливостей внаслідок об'єднання компонентів.

3.3.2 Складовий рівень довіри А (СПД-А).

Що передбачає структурну композицію

СПД-А застосовуємо, коли складова ОО інтегрована і потрібно впевненість в коректності безпечного функціонування результуючої композиції. Це вимагає взаємодії (кооперації) з розробником залежного компонента з питань отримання інформації по проекту і результатів тестування з матеріалів сертифікації залежного компонента без залучення розробника базового компонента.

Тому СПД-А застосуємо в тих випадках, коли розробникам або користувачам потрібно незалежно підтверджений рівень довіри до безпеки

від низького до помірного при відсутності прямої доступності повної інформації про розробку.

Аналіз підтриманий незалежним тестуванням інтерфейсів базового компонента, на які покладаються залежні компоненти, як описано в інформації про залежності, свідоцтві тестування розробником, що базується на інформації про залежності, інформації по розробці і обґрунтуванні композиції, а також вибірковим незалежним підтвердженням результатів тестування, виконаного розробником. Аналіз також підтриманий проведеним оцінювачем коротким аналізом вразливостей складеного ОО.

СПД-А також забезпечує довіру шляхом унікальної ідентифікації складеного ОО.

Таблиця 3.9 - Складовий рівень довіри А

клас довіри	компоненти довіри
ACO: Композиція	ACO_COR.1 Обгрунтування композиції
	ACO_CTT.1 Тестування інтерфейсів
	ACO_DEV.1 Функціональне опис
	ACO_REL.1 Базова інформація про залежності
	ACO_VUL.1 Короткий аналіз вразливостей композиції
AGD: Керівництва	AGD_OPE.1 Керівництво користувача по експлуатації
	AGD_PRE.1 Підготовчі процедури

Продовження таблиці 3.9 - Складовий рівень довіри А

ALC: Підтримка життєвого циклу	ALC_CMC.1 Маркування ОО
	ALC_CMS.2 Охоплення КК частин ОО
ASE: Оцінка завдання з безпеки	ASE_CCL.1 Твердження про відповідність
	ASE_ECD.1 Визначення розширених компонентів
	ASE_INT.1 Введення ЗБ
	ASE_OBJ.1 Цілі безпеки для середовища функціонування
	ASE_REQ.1 Встановлені вимоги безпеки
	ASE_TSS.1 Коротка специфікація ОО

3.3.3 Складовий рівень довіри В (СПД-В)

Що передбачає методичну композицію.

СПД-В дозволяє сумлінному розробнику досягти максимальної довіри на основі розуміння на рівні підсистем впливу взаємозв'язків між ОО-компонентами, що включаються в складову ОО, при мінімальній залежності від залучення розробника базового компонента.

СПД-В застосуємо в тих випадках, коли розробникам або користувачам потрібно незалежно підтверджений помірний рівень довіри до безпеки на основі всебічного дослідження складеного ОО і процесу його розробки без істотного реінжинірингу (відновлення процесу проектування).

Аналіз підтриманий незалежним тестуванням інтерфейсів базового компонента, на які покладаються залежні компоненти, як описано в інформації про залежності (яка для даного СПД також включає проект

ОО), свідоцтві тестування розробником, що базується на інформації про залежності, інформації по розробці і обґрунтуванні композиції ОО, а також вибірковим незалежним підтвердженням результатів тестування, виконаного розробником. Даний аналіз також підтриманий проведеним оцінювачем аналізом вразливостей складеного ОО, що демонструє протистояння порушнику з Базовим потенціалом нападу.

Цей СПД демонструє значне збільшення рівня довіри в порівнянні з СПД-А, вимагаючи більш повного охоплення тестуванням функціональних можливостей безпеки.

Таблиця 3.10- Складовий рівень довіри В

клас довіри	компоненти довіри
ACO: Композиція	ACO_COR.1 Обгрунтування композиції
	ACO_CTT.2 Суворе тестування інтерфейсів
	ACO_DEV.2 Базове свідоцтво за проектом
	ACO_REL.1 Базова інформація про залежності
	ACO_VUL.2 Аналіз вразливостей композиції
AGD: Керівництва	AGD_OPE.1 Керівництво користувача по експлуатації
	AGD_PRE.1 Підготовчі процедури
ALC: Підтримка життєвого циклу	ALC_CMC.1 Маркування ОО
	ALC_CMS.2 Охоплення КК частин ОО

Продовження таблиці 3.10 - Складовий рівень довіри B

ASE: Оцінка завдання з безпеки	ASE_Утвердження про відповідність
	ASE_ECD.1 Визначення розширених компонентів
	ASE_INT.1 Введення ЗБ
	ASE_OBJ.2 Цілі безпеки
	ASE_REQ.2 Похідні вимоги безпеки
	ASE_SPD.1 Визначення проблеми безпеки
	ASE_TSS.1 Коротка специфікація ОО

3.3.4 Складовий рівень довіри C (СПД-С).

Що передбачає методичну композицію, тестування і перевірку.

СПД-С дозволяє розробнику досягти максимальної довіри на основі точного аналізу взаємозв'язків між компонентами складеного ОО, який незважаючи на суворість не вимагає повного доступу до всіх свідченнями базового компонента.

Аналіз підтриманий незалежним тестуванням інтерфейсів базового компоненту, на які покладаються залежні компоненти, як описано в інформації про залежності (яка для даного СПД також включає проект ОО), свідоцтво тестування розробником, що базується на інформації про залежності, інформації по розробці і обґрунтуванні композиції ОО, а також вибірковим незалежним підтвердженням результатів тестування, виконаного розробником. Даний аналіз також підтриманий проведеним оцінювачем аналізом вразливостей складеного ОО, що демонструє протистояння порушнику з посиленим базовим потенціалом нападу.

Цей СПД дає значне збільшення рівня довіри в порівнянні з СПД-В, вимагаючи більшого опису проекту і демонстрацію протистояння порушникам з більш високим потенціалом нападу.

Таблиця 3.11 - Складовий рівень довіри С

клас довіри	компоненти довіри
ACO: Композиція	ACO_COR.1 Обгрунтування композиції
	ACO_CTT.2 Суворе тестування інтерфейсів
	ACO_DEV.3 Детальне свідоцтво за проектом
	ACO_REL.2 Інформація про залежності
	ACO_VUL.3 Посилений базовий аналіз вразливостей композиції
AGD: Керівництва	AGD_OPE.1 Керівництво користувача по експлуатації
	AGD_PRE.1 Підготовчі процедури
ALC: Підтримка життєвого циклу	ALC_CMC.1 Маркування ОО
	ALC_CMS.2 Охоплення КК частин ОО
ASE: Оцінка завдання з безпеки	ASE_CCL.1 Твердження про відповідність
	ASE_ECD.1 Визначення розширених компонентів
	ASE_INT.1 Введення ЗБ
	ASE_OBJ.2 Цілі безпеки
	ASE_REQ.2 Похідні вимоги безпеки
	ASE_SPD.1 Визначення проблеми безп
	ASE_TTS.1 Коротка специфікація ОО

3.4 Аналіз класів довіри

3.4.1 Клас APE: Оцінка профілю захисту

Оцінка ПЗ потрібна для демонстрації того, що ПЗ є повним, несуперечливим і правильним, а в разі, якщо ПЗ ґрунтується на одному або декількох інших ПЗ або пакетах довіри, що цей ПЗ є коректною реалізацією цих ПЗ і пакетів довіри. Ці властивості необхідні для того, щоб ПЗ можна було використовувати в якості основи для розробки ЗБ або іншого ПЗ.

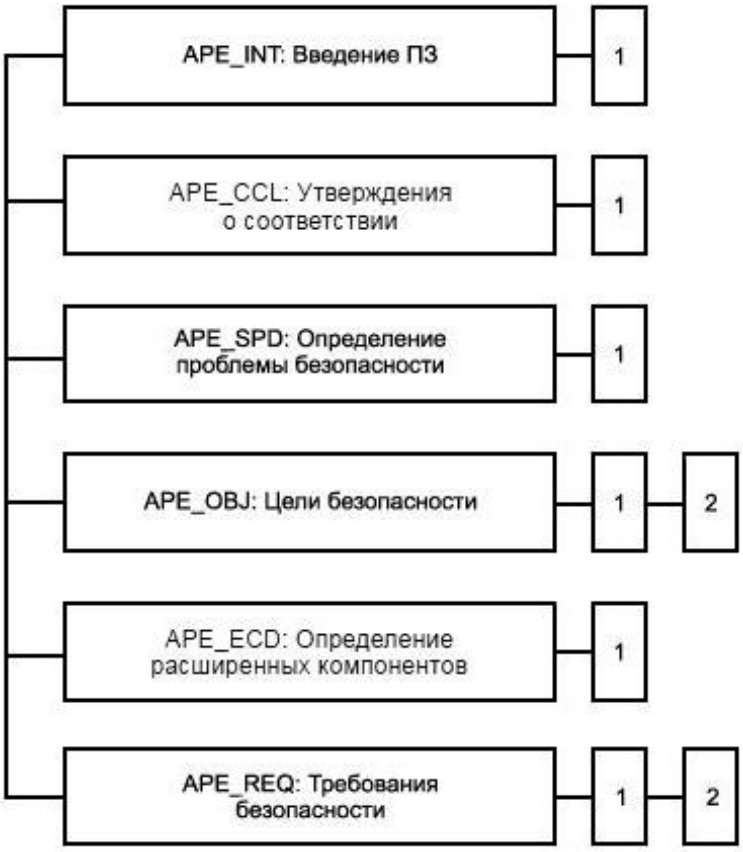

Рисунок 3.4.1 Декомпозиція класу APЄ "Оцінка профілю захисту"

3.4.2 Клас ASE: Оцінка завдання з безпеки

Оцінка ЗБ потрібна для демонстрації того, що ЗБ є правильним і внутрішньо несуперечливим, і якщо ЗБ засноване на одному або більше ПЗ або пакетах довіри, що ЗБ є коректною реалізацією цих ПЗ і пакетів. Ці властивості необхідні для того, щоб можна було використовувати ЗБ в якості основи при оцінці ОО.

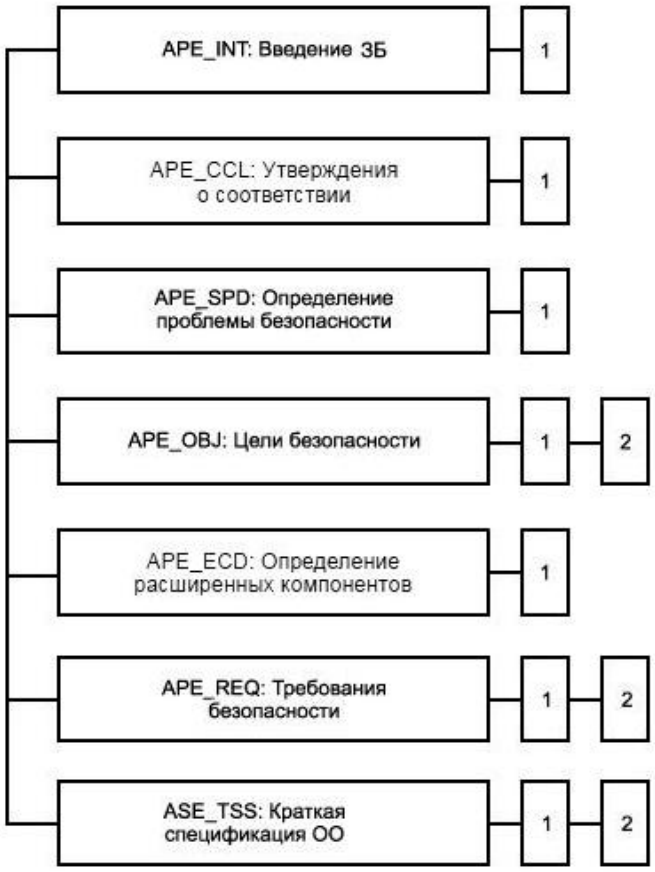

Рисунок 3.4.2 Декомпозиція класу ASE "Оцінка ЗБ"

3.4.3 Клас ADV: Розробка

Вимоги класу "Розробка" надають інформацію про об'єкт оцінки. Відомості, отримані шляхом вивчення цієї інформації, служать основою

для проведення аналізу вразливостей і тестування ОО відповідно до опису, представленим в класах AVA "Аналіз вразливостей" і ATE "Тестування".

Клас "Розробка" містить шість сімейств довіри для структурування та подання ФБО на різних рівнях деталізації.

3.4.4 Клас AGD: Керівництва

Клас "Керівництва" надає вимоги до документації посібників для всіх призначених для користувача ролей. Для безпечної підготовки і безпечного функціонування ОО необхідно описати всі істотні аспекти, які стосуються безпечного застосування ОО. В даному класі також розглядаються випадки ненавмисних неточностей конфігурації або помилок експлуатації ОО.

У багатьох випадках доречно надання окремих посібників з підготовчими процедурами і експлуатації ОО або навіть окремих посібників для різних призначених для користувача ролей: кінцевих користувачів, адміністраторів, програмістів-розробників додатків, що використовують програмні і апаратні інтерфейси і т.д.

Клас "Керівництва" підрозділяється на два сімейства: що стосується керівництва користувача по підготовчим процедурам і керівництва користувача по експлуатації.

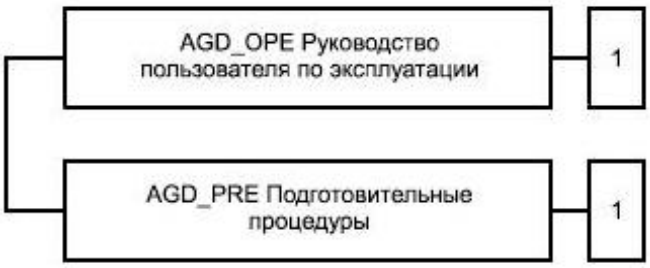

Рисунок 3.4.4 - Декомпозиція класу AGD "Керівництва"

3.4.5 Клас ALC: Підтримка життєвого циклу

Підтримка життєвого циклу є аспектом встановлення організаційного порядку і управління в процесі вдосконалення ОО під час його розробки і супроводу. Впевненість у відповідності ОО вимогам безпеки до ОО буде більшою, якщо аналіз безпеки і формування свідчень виконуються на регулярній основі як невід'ємна частина діяльності по розробці і супроводу.

В життєвому циклі продукту визначається, під чиєю відповідальністю знаходиться ОО - розробника або користувача, а не те, чи розташований він в призначеній для користувача середовищі або середовищі розробки. Перехідним моментом є момент передачі ОО користувачеві. Це також момент переходу від вимог класу ALC "Підтримка життєвого циклу" до вимог класу AGD "Керівництва".

До складу класу ALC "Підтримка життєвого циклу" входять сім родин. Сімейство "Визначення життєвого циклу" (ALC_LCD) містить вимоги до опису верхнього рівня життєвого циклу ОО; сімейство "Можливості КК" (ALC_CMC) містить вимоги до більш докладного опису управління елементами конфігурації. У сімействі "Область КК" (ALC_CMS) представлені вимоги до мінімального набору засобів конфігурації для належного управління елементами конфігурації. Сімейство "Безпека розробки" (ALC_DVS) включає вимоги до фізичних, процедурних, організаційних заходів безпеки та іншими критеріями безпеки; сімейство "Інструментальні засоби і методи" (ALC_TAT) включає вимоги до інструментальних засобів розробки і виконання стандартів реалізації, використовуваних розробником; сімейство "Усунення недоліків" (ALC_FLR) включає вимоги по обробці недоліків

безпеки. Сімейство "Поставка" (ALC_DEL) визначає вимоги до процедур, використовуваним при поставці ОО споживачеві. [9]

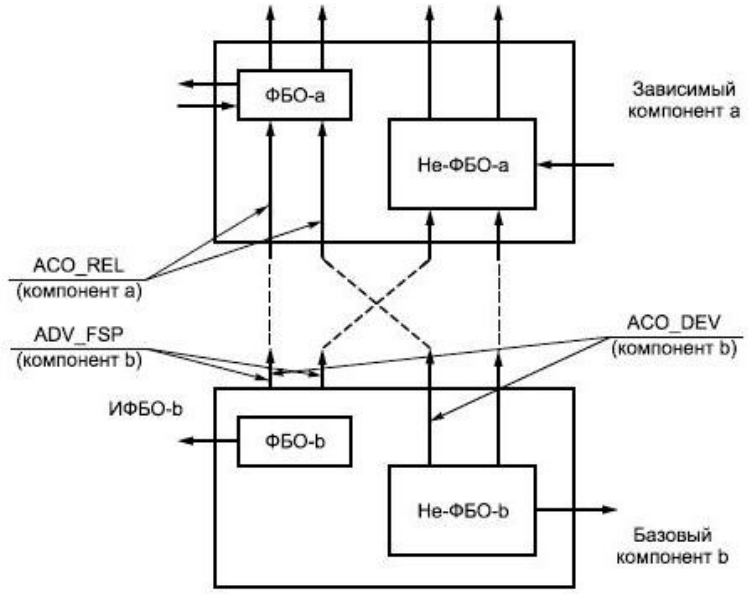

Рисунок 3.4.8 - Взаємозв'язок між родинами ACO і взаємодіями між компонентами

3.5 Висновкі до розділу 3

Компоненти довіри до безпеки, які визначені в ISO / IEC 15408-3, є основою для вимог довіри до безпеки, що відображаються в профілі захисту (ПЗ) або в завданні з безпеки (ЗБ).

Ці вимоги встановлюють стандартний спосіб вираження вимог довіри для ОО. ISO / IEC 15408-3 є каталог компонентів, сімейств і класів довіри. В ISO / IEC 15408-3 також визначені критерії оцінки для ПЗ і ЗБ і представлені оціночні рівні довіри для зумовленої в ISO / IEC 15408 шкали довіри до ГО, яка називається Оціночні рівні довіри (Оуд).

Потенційні користувачі даного міжнародного стандарту включають споживачів, розробників і оцінювачів безпечних продуктів IT. В ISO / IEC 15408-1 надана додаткова інформація про цільову аудиторію

ISO / IEC а також по використанню ISO / IEC 15408 окремими групами осіб, складовими цільова аудиторія. Ці групи можуть використовувати дану частину ISO / IEC 15408 наступним чином:

a) Споживачі можуть використовувати дану частину ISO / IEC 15408 при виборі компонентів для вираження вимог довіри, щоб задовольнити цілі безпеки, відображені в ПЗ або ЗБ, і при визначенні необхідних рівнів довіри до безпеки ОО;

b) Розробники, які при виробництві ОО враховують існуючі або передбачувані вимоги безпеки споживачів, можуть звернутися до ISO / IEC 15408-3 при інтерпретації викладу вимог довіри і при визначенні підходів до забезпечення довіри до ОО;

c) Оцінювачі можуть використовувати вимоги довіри, певні в ISO / IEC 15408-3, як обов'язкове виклад критеріїв оцінки при визначенні довіри до ОО, а також при оцінці ПЗ і ЗБ.

ВИСНОВКИ

1) Інформаційна безпека (англ. Information Security, а також - англ. InfoSec) - практика запобігання несанкціонованому доступу, використання, розкриття, спотворення, зміни, дослідження, записі або знищення інформації. Це універсальне поняття застосовується незалежно від форми, яку можуть приймати дані (електронна, або наприклад, фізична). Основне завдання інформаційної безпеки - збалансована на захист конфіденційності, цілісності і доступності даних з урахуванням доцільності застосування і без будь-якої шкоди продуктивності організації. Це досягається, в основному, за допомогою багатоетапного процесу управління ризиками, який дозволяє ідентифікувати основні засоби та нематеріальні активи, джерела загроз, уразливості, потенційну ступінь впливу і можливості управління ризиками. Цей процес супроводжується оцінкою ефективності плану з управління ризиками.

2) Оцінка інформаційної безпеки базується на моделях системи безпеки, що складаються з перерахованих в стандарті функцій. В ISO 15408 міститься ряд зумовлених моделей (так званих профілів), що описують стандартні модулі системи безпеки. З їх допомогою можна не створювати моделі поширених засобів захисту самостійно, не винаходжуючи велосипед, а користуватися вже готовими наборами описів, цілей, функцій і вимог до цих коштів. Простим прикладом профілів може служити модель СУБД.

3) Сертифікований профіль являє собою повний опис певної частини (або функції) системи безпеки. У ньому міститься аналіз внутрішнього і зовнішнього середовища об'єкта, вимоги до його функціональності і надійності, логічне обгрунтування його використання, можливості та обмеження розвитку об'єкта.

4) Стандарт ISO 15408 вигідно відрізняє відкритість. Описує ту чи іншу область системи безпеки профіль можна створити самостійно за допомогою розробленої в ISO 15408 структури документа. У стандарті визначено також послідовність дій для самостійного створення профілів.

5) Функції системи інформаційної безпеки забезпечують виконання вимог конфіденційності, цілісності, достовірності та доступності інформації. Всі функції представлені у вигляді чотирирівневої ієрархічної структури: клас - сімейство - компонент - елемент. За аналогією представлені вимоги якості. Подібна градація дозволяє описати будь-яку систему інформаційної безпеки і зіставити створену модель з поточним станом справ. У стандарті виділені 11 класів функцій: аудит, ідентифікація і аутентифікація, криптографічний захист, конфіденційність, передача даних, захист призначених для користувача даних, управління безпекою, захист функцій безпеки системи, використання ресурсів, доступ до системи, надійність засобів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1) Погребняк А. В. Технології комп’ютерної безпеки: монографія / А. В. Погребняк– Рівне : МЕГУ, 2011. – 117 с.

2) НД ТЗІ 1.1-003-99 Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу.

3) НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

4) НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.

5) ISO/IEC 15408-1:2009 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model.

6) ISO/IEC 15408-2:2008 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components.

7) ISO/IEC 15408-3:2008 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components

8) Про внесення змін до наказу Міністерства юстиції України, Адміністрації Державної служби спеціального [...] Мін'юст України, Адміністрація Держспецзв’язку; Наказ, Перелік від 25.12.2014 № 2170/5/703.

9) International Organization for Standardization [Електронний ресурс]// – Режим доступу: http://www.iso.org/iso/home.html.